CA Service Desk Manager

Guia de Administração

Release 12.7.00

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos CA Technologies:

- CA Asset Portfolio Management (CA APM)
- CA CMDB
- CA Business Intelligence
- CA BSI (CA Business Service Insight)
- CA Configuration Automation (anteriormente conhecido como CA Cohesion ACM)
- CA EEM
- CA EWA (CA Enterprise Workload Automation)
- CA Process Automation (anteriormente conhecido como CA IT PAM)
- CA Management Database (CA MDB)
- CA Management Portal
- CA NSM (CA Network and Systems Management)
- Portal da CA
- CA RCM (CA Remote Control Manager)
- CA SDM (CA Service Desk Manager)
- CA Service Management
- CA SiteMinder
- CA Software Delivery
- Gerenciador de infraestrutura CA Spectrum® (CA Spectrum® Infrastructure Manager)
- CA Wily
- CA Workflow

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Índice

Capítulo 1: Introdução 29

Público-alvo ... 29
O que você necessita saber ... 29
Processos e práticas recomendadas para gerenciamento de serviços ... 30

Capítulo 2: Gerenciando servidores 31

Número de servidores ... 31
Tarefas de configuração do servidor ... 32
Configurando o TCP/IP ... 33
Alterar a configuração de um servidor ... 34
Configuração do ITIL ... 34
    Disciplinas do serviço ITIL ... 35
    Opções de Interface de funcionário e convidado ... 36
    Segurança de log de atividade ... 38
Interface PDA ... 40
Suporte do Tablet ... 41
Interface de usuário móvel de exemplo do REST ... 42
    Implantar o interface de usuário móvel de exemplo do REST ... 44
    Ativar a interface de usuário móvel de exemplo do REST ... 48
    Exemplo: página inicial da interface do analista ... 49
    Exemplo: o analista pesquisa um incidente ... 50
    Exemplo: o analista cria um incidente ... 50
    Exemplo: o analista registra um Comentário somente para uso interno ... 51
    Exemplo: página inicial da interface do funcionário ... 53
    Exemplo: o funcionário cria um incidente ... 54
    Exemplo: o funcionário Edita um incidente ... 54
Log do Tomcat ... 55
    Padrões do servlet ... 56
    Relatórios do REST ... 56
    Ativar o log CXF ... 57
Iniciar um servidor secundário ... 57
Iniciar o servidor primário ... 58
Status do servidor ... 60
Configurar SSL no Tomcat ... 61

Configurar um servidor secundário do Pintor de telas da web 62
Como implantar serviços web de CMDBf 63
Para um servidor (Windows) 63
Parar um servidor (UNIX) 64

Capítulo 3: Definindo a estrutura comercial 65

Como definir a estrutura comercial 65
- Contatos 66
- Grupos 66
- Sites 67
- Locais 67
- Organizações 67

Definir a infra-estrutura comercial 68
- Requisição de definição de objetos 69
- Famílias e classes 69
- Fabricantes e modelos 70
- Status do serviço 70
- Tipos de fornecedor e fornecedores 70
- Itens de configuração 71
- Ferramentas externas de gerenciamento de ativos 72

Multi-locação 72
- Provedor de serviços 73
- Como funciona a Multilocação 74
- Impacto na interface com o usuário 82
- Impacto no Support Automation 86
- Impacto do Gerenciamento de conhecimento 87
- Como usar a Multilocação 89

Capítulo 4: Implementando políticas 101

Implementação de diretivas 101
Notificações 101
- Associações de atividades 102
- Notificações de atividade 103
- Notificações de contatos de objeto 105
- Métodos de notificação 106
- Notificações de email 109
- Regras de notificação 114
- Exemplo: criar um modelo de mensagem 125

Objetos em mensagens ... 127
Códigos e frases de notificações ... 128
Lista de destinatários de notificação manual ... 132
Notificações para responsável anterior ... 133
Notificações de item de configuração ... 136
Notificações de pesquisa ... 137
Como adicionar hiperlinks de URL a notificações ... 138
Leitor de logs de notificação ... 139
Administração de email ... 143
Caixas de correio ... 144
Regras de caixa de correio ... 145
Políticas de caixa de correio ... 154
Como implementar caixas de correio ... 156
Várias caixas de correio ... 162
Como configurar respostas de emails ... 164
Objetos ... 166
Considerações sobre uso de objetos ... 167
Proteção e segurança de artefatos ... 169
Contratos de nível de serviço ... 170
Utilização do SLA ... 171
Processamento do SLA clássico ... 172
Tipos de serviço e eventos ... 172
Como implementar tipos de serviço ... 173
Tipos de serviço predefinidos ... 174
Configuração de eventos ... 175
Como criar Metas de serviço ... 177
Contratos de serviço ... 178
Migração de contratos de serviço ... 180
Horário para violação ... 180
Fusos horários e turnos de trabalho ... 181
Segurança ... 185
Configurações da base de usuários CA EEM e CA Workflow ... 186
Considerações de segurança ... 197
Autenticação CA EEM para o CA Process Automation ... 198
Autenticação de usuário ... 199
Como o CA SDM autentica usuários ... 199
Autenticação externa ... 200
Tipos de validação ... 201

Contagens de usuários conectados e usuários licenciados 202
Logs internos 203
Integração do CA SDM 203
Associações de partições de dados 203
Partições de dados 204
Configuração da partição de dados 204
Especificações da restrição 205
Tipos de restrição 206
Criar uma restrição de partição de dados para atribuições do CAB 208
Configure as restrições da partição de dados do Gerenciamento de conhecimento para permissões com base em função 209
Pesquisas 210
Configurar seu sistema para pesquisas 210
Preparar uma pesquisa 210
Definir notificações de pesquisa 211
Criando relatórios da pesquisa 212
Pesquisa gerenciada 213
Web Services 213

Capítulo 5: Configurando contas de usuário 215

Contatos 215
Definições de contato 215
Grupos 217
Tipos de contato 218
Determinar o comportamento de acordo com o tipo de contato 218
Configuração de notificação com base no tipo de contato 218
Selecionar contatos de acordo com o tipo de contato 219
Tipos de tratamento especiais 219
Como configurar contatos de tratamento especial 220
Associar um contato a um tipo de tratamento especial 221
Dados no diretório LDAP 222
Configurar opções de LDAP 223
Verifique a integração LDAP 226
Criar um contato automaticamente 229
Atribuições de tipo de acesso a partir de grupos LDAP 229
Importação em lote de contatos usando dados LDAP 230
Atualização em lote de contatos usando dados LDAP 233
Autenticação LDAP 236

Transport Layer Security 236
Mapeamento de atributo 237
Solução de problemas 238

Capítulo 6: Gerenciando funções 251

Funções 251
Funções predefinidas 251
Segurança baseada em funções 254
Como funcionam os tipos de acesso 254
Registros de função 258
Áreas de acesso funcional 259
Partições de dados 264
Navegação com base em função 264
Guias 265
Guias predefinidas 267
Formulários web 269
Grupos de formulários 270
Árvores de menus 270
Recursos de árvores do menu 272
Barras de menu 272
Barras de ferramentas 274
Recursos Ir 274
Pacotes de ajuda 275
Como implementar uma função personalizada 275
Como implementar uma árvore de menu personalizada 277
Criar um registro de função 279
Criar um registro de guia 280
Criar um registro de barra de menu 281
Criar um registro de formulário Web 282
Copiar uma árvore de menus 283
Criar e personalizar uma árvore de menu 284
Criar e publicar um pacote de ajuda 286
Alternar funções 288

Capítulo 7: Estabelecendo estrutura de suporte 289

Estrutura de suporte 289
Modelos 290
Modelo interno 290

Modelo externo 291
Modelo combinado 292
CA Workflow 293
Workflow em Tempo de execução 294
Selecione uma definição de processo de fluxo de trabalho 295
Tarefas de fluxo de trabalho 296
Integração do fluxo de trabalho do CA Process Automation 297
Componentes do CA Process Automation 298
Integração do CA Process Automation com CA SDM em tempo de execução 299
Como criar uma definição de processo 300
Criar um formulário de solicitação inicial 301
Anexar uma definição de processo do CA Process Automation 303
Códigos compartilhados 304
Códigos de prioridade 305
Códigos de gravidade 306
Códigos de impacto 306
Códigos de urgência 306
Códigos de status 307
Códigos de status de solicitação 308
Códigos de status de requisição de mudança 309
Códigos de status da ocorrência 311
Códigos de status da tarefa 312
Tipos de tarefa 313
Acompanhamento de incidente 314
Instalar acompanhamento de incidente 315
Solicitação/Incidente/Áreas de problemas 316
Propriedades de Área de solicitação/incidente/problema 318
Definir áreas de solicitação/incidente/problema para autoatendimento 320
Categorias requisições de mudança e ocorrência 321
Categorias de mudança predefinidas 322
Categorias de ocorrência predefinidas 322
Regras para alterar categorias em um ticket 322
Propriedades de categorias 323
Defina as categorias de mudança e ocorrência para um autoatendimento 326
Fechamento automático de tickets 327
Como definir configurações de ticket de fechamento automático 328
Como definir uma notificação de atividade de fechamento automático 329
Atividades de ticket relacionadas 329

Como definir notificações de atividade para tickets relacionados ... 331
Como definir notificações de atividade de ticket relacionadas ... 332
Cálculo de prioridade ... 332
Como o cálculo de prioridade gerencia valores de ticket ... 334
O cálculo de prioridade gera valor de urgência depois de salvar tickets de autoatendimento ... 337
Como definir o cálculo de prioridade ... 338
Transições de status e controles de atributos dependentes ... 351
Trabalhar com transições de status e Controles de atributos dependentes ... 352
Configurar transições de status ... 352
Configurar controles de atributos dependentes ... 354
Métodos de serviços web ... 355
Fluxos de transição predefinidos ... 356
Melhor prática: Transições de status predefinidas ... 360
Transições de status para autoatendimento ... 362
Como as transições para autoatendimento funcionam ... 363
Como criar ou atualizar tipos de transição para transições ... 364
Como vincular tipos de transição a transações ... 364
Ativar tipos de transição predefinidos ... 365
Timers ... 367
Fusos horários ... 368
Acionadores de evento de tipo de serviço ... 368
Acionadores de evento de fuso horário ... 369
Regras de fuso horário ... 370
Anexos de arquivo ... 371
Fazer upload e download de anexos de arquivo ... 372
Repositórios ... 372
Anúncios ... 376
Visibilidade interna do anúncio ... 377
Especificar a urgência do anúncio ... 377
Configuração de consultas armazenadas ... 377
Números de sequência ... 379
Uso do log de auditoria ... 380
Integração com o CA Network and Systems Management ... 380

Capítulo 8: Controlando o comportamento do sistema 381

Uso do Gerenciador de opções ... 381
Como modificar o ambiente do sistema ... 382
Eventos ... 383

Macros 383
Tipos de macro 384
Usar macros com eventos 385
Usar macros no comportamento de ocorrências e categorias de mudança 386
Usar macros com notificação múltipla 386
Usar macros com condições definidas pelo local 387

Capítulo 9: Configurando a interface da Web 389

Configuração da interface da Web 389
Como a interface da web funciona 389
Web Director e distribuição de carga da web 390
Web.cfg e CA SDM 391
Atribuir um mecanismo da Web a um WebDirector 392
Defina a função do mecanismo da Web com parâmetros do Web Director 393
Ambiente sem SSL com equilíbrio de carga de trabalho básico 393
Ambiente com SSL global com equilíbrio de carga de trabalho básico 394
logon direcionado em um ambiente sem SSL com equilíbrio de carga de trabalho opcional 394
Logon SSL direcionado em ambiente misto com equilíbrio de carga de trabalho opcional 395
Configuração de web directors e de mecanismos da web 396
Como implementar um ambiente de logon SSL com somente um servidor primário 397
Como criar um sistema somente com um servidor primário 398
Verificar os valores de parâmetros do web director 401
Os mecanismos da Web de logon seguro devem residir no diretório físico mapeado ao diretório virtual com proteção SSL (nesse caso, 'CAisdsec'). 402
Servidores secundários e recursos da web 403
Como preparar recursos da web 403
Como criar um sistema com servidores secundários 404
Configuração do servidor 407
Fazer mudanças usando pdm_edit.pl 420
Iniciar o web director 425
Como o web director lida com sessões de usuário 426
Melhorar o desempenho com o armazenamento em cache no navegador 428
Configure o Microsoft Internet Information Server 428
Configurar Apache 429
Limpar o cache 430
Registrar o comportamento de bloqueio na interface da Web 431
Imprimir páginas da Web do CA SDM 432
Modificação de arquivo de configuração 432

SchedExpMaximum 443
SelListCacheExclude 443
SelListCacheMax 443

Capítulo 10: Configurando atribuição automática 449

Atribuição automática 449
Relacionamentos de atribuição automática 450
Métodos de atribuição automática 450
Como começar a implementação da atribuição automática 451
Áreas e categorias 452
Grupos de analista 452
Analistas 453
Como atribuir automaticamente tickets a um grupo e não aos contatos do grupo 454
Atribuição automática por local 455
Atribuição automática por turno de trabalho 456
Grupo e responsável padrão 458
Ativação da atribuição automática 459
Substituição da atribuição automática 460
Controles de atribuição 461
Atribuição manual 461
Opção de definição de responsável 462
Iss assignee_set 462
Area_Defaults 462
Opções de responsável e grupo obrigatórias 462
Modelos 464
Interface do CA Network and Systems Management 464
Registro de atividades 464
Ativar o Log de atividade para atributos adicionais 465
Rastreamento de atribuição automática 465
Consultas armazenadas 466
Como a atribuição automática atribui tickets 466
Como a atribuição automática atribui tarefas do fluxo de trabalho 474
Atribuições automáticas com base em item de configuração 477
Como funciona a atribuição automática com base em item de configuração 477
Habilitar atribuições automáticas com base em item de configuração 481

Capítulo 11: Gerenciando seu banco de dados 483

Utilitários de gerenciamento de banco de dados 483

Selecione e configure o banco de dados ... 483
Carregamento de banco de dados ... 484
Como criar e usar um arquivo de entrada ... 485
Eliminar e restaurar restrições ... 486
Backup do banco de dados ... 487
Restauração do banco de dados ... 487
Substituição da tabela do banco de dados ... 488
Extração de dados ... 488
Usar o extrator de dados em UNIX ... 489
Seleção de dados para extração ... 489
Retirada de referência de dados ... 490
Exemplo de como usar pdm_deref ... 491
Usar o modo Dbadmin ... 493
Regras de arquivamento e eliminação ... 494
Executar regras de arquivamento e eliminação ... 495
Exibir regras de arquivamento e eliminação ... 496
Iniciar arquivamento e eliminação usando um agendador de terceiros ... 497
Definições de regras de arquivamento e eliminação ... 497
Histórico de arquivamento e eliminação ... 500
Tratamento de anexos (arcpur) ... 502
Como restaurar dados arquivados ... 504
Arquivar e eliminar dados do KPI ... 505
Fóruns do Gerenciamento de conhecimento sobre arquivamento e eliminação ... 506

Capítulo 12: Usando a API de texto 509

API de texto ... 509
Interface de linha de comando ... 510
Interface do CA Network and Systems Management ... 510
Formato de entrada ... 511
Palavras-chave ... 512
Convenções de entrada de palavra-chave ... 515
Formatar uma mensagem de email para atualizar um ticket ... 516
Delimitadores de início e final de mensagens de email ... 517
Como a API de texto usa objetos ... 517
Como configurar respostas de notificação para atualizar tickets ... 518
Métodos de conversão ... 522
O arquivo de configuração ... 524
Opções ... 525

Padrões ... 525
Ignorar entrada ... 526
Entrada de exemplo ... 527

Capítulo 13: Gerenciando controle de versão 529

Como funciona o controle de versão ... 529
Arquivos de controle de versão ... 530
Arquivos de controle do servidor primário ... 530
Arquivos de controle do servidor secundário e cliente ... 531
Controle de versão para personalizações de instalação ... 532
Modos de servidor de controle de versão ... 533
Sintaxe do arquivo de controle de versão ... 534
Parâmetros de controle de versão ... 535
Remover o controle de um componente ... 540

Capítulo 14: Gerenciamento de itens de configuração 541

Usando a interface da Web ... 541
Exibir itens de configuração ... 542
Criar um item de configuração ... 543
Atualizar um item de configuração ... 543
Associar uma janela de manutenção a um IC ... 544
Exibir janelas de mudança associadas ... 545
Exibir o histórico do item de configuração ... 545
Desativar um item de configuração ... 545
Reativar um item de configuração ... 546
ICs Contato, Local e Organização ... 546
Criar um IC a partir de um objeto básico ... 547
Selecionar um objeto base para um IC ... 548
Editar detalhes do IC de um objeto base ... 548
Editar atributos do IC de um objeto base ... 549
Criar IC de um objeto base usando o GRLoader ... 550
Relacionamentos do CI ... 550
Tipos de relacionamentos de ICs ... 551
Criar um tipo de relacionamento ... 552
Gerenciar um relacionamento de IC ... 553
Criar um relacionamento de IC ... 553
Exibir relacionamentos de um IC ... 554
Desativar um relacionamento de IC ... 554

Reativar um relacionamento de IC ... 555
Desativar Relacionamentos do IC (Editar na lista) ... 555
Desativar um relacionamento de IC usando o GRLoader ... 556
Reativar um relacionamento de IC usando o GRLoader ... 557
Excluir um relacionamento de IC do banco de dados ... 558
Comparação e histórico de relacionamento do IC ... 559
Versão ... 559
Usos do Versioning ... 561
Ativo compartilhado e registros de trilha de auditoria de IC ... 562
Terminologia de versões ... 563
Origens de dados de versão ... 566
Integração do gerenciamento de mudança do CA SDM ... 567
Integração do CA APM ... 568
Gerenciamento de controle de versão de IC ... 569
Gerenciamento de mudança do CA SDM ... 588
Exibir atributos de IC em outros produtos CA ... 589
Usando o visualizador do CMDBf ... 590
CMDB Visualizer ... 590
Realizar análise da causa raiz ... 593
Administração do Visualizer ... 593
Adicionar um ativo detectado ... 594
Sinalizadores Ativo e IC ... 595
CI Reconciliation ... 597
Reconciliação com base em MDR ... 598
Como identificar e resolver ICs ambíguos ... 600
Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) ... 614
Gerenciar Transações armazenadas temporariamente ... 620
Área de trabalho de transação ... 621
Preenchendo a área de trabalho de transação ... 623
Como usar a interface da Web para atualizar dados na TWA ... 636
Gerenciar transações de relacionamento ... 639
Como carregar transações para o CMDB ... 641
Administração da TWA ... 643
Manutenção de dados do CA CMDB ... 647
Estrutura de classe /família do CA CMDB ... 648
Alterar família/classe de um único IC ... 649
Alterar a família/classe de uma lista de ICs ... 649
Alterar a família/classe do IC usando o GRLoader ... 650

Extensão do CA CMDB 650
CACF (Configuration Audit and Control Facility) 663
Administração e definição de política do CACF 665
Atributos gerenciados 682
Estados de mudança gerenciada 682
Especificações de mudança 685
Como uma verificação de mudança ocorre 691
Como arquivar e limpar os dados de auditoria 697
Implementar uma estratégia de verificação de mudanças 698
Planejamento e implementação de verificação de mudança 703
Melhores práticas de verificação de mudanças 711
Verificar a Atualização do valor do atributo do IC manualmente 715
Exemplo: Permitir Atualizações informais somente a partir de um Local específico 720
Exemplo: Atualizar laptops na organização 722
Exemplo: Bloquear requisições de mudança não verificados 723
Exemplo: permitir uma Atualização de IC se não houver requisição de mudança correspondente 724
Exemplo: adiar todas as atualizações do CA Configuration Automation para a TWA 724
Exemplo: Registrar somente os Resultados da política como um teste 725
Exemplo: Rejeitar uma atualização de IC 725
Exemplo: Permitir requisições de mudança criadas sem especificações 726
Exemplo: Não permitir requisições de mudança criadas sem especificações 727
Exemplo: permitir inserções informais de fontes selecionadas 727
Exemplo: permitir uma atualização informal de um IC que não seja de produção 728

Capítulo 15: Administração de MDRs 729

O que é um MDR? 729
Classes e nomes de MDRs 730
Como o MDR complementa o CA SDM? 730
Definição de MDR para o CA SDM 731
MDR Launcher 731
Definir um URL para iniciar um MDR 732
Configurar um MDR como provedor do CA APM 734
Execução em contexto do CA CMDB para o CA APM 735
Propriedades de ICs que oferecem suporte à federação do MDR 735
ID do ativo federado 735
Nome do MDR 736
Classe do MDR 736

Definição de MDRs com instalação do CA Cohesion ACM 737
MDRs do CA Cohesion ACM 738
Como associar um MDR a um IC manualmente 739
Importação automática do CA Cohesion 740
IC para mapeamento do MDR 740
Administração da definição de MDR 742
Relatório do CA Cohesion ACM 742
Usando o GRLoader 743
Convenções e restrições de nomenclatura de ICs 743
Convenção de nomenclatura de system_name 745
Usando o visualizador do CMDBf 746
Como atualizar arquivos de metadados para mapeamento do CMDBf 747
Como exibir valores de atributos do MDR com nomes de atributos do CA CMDB 749
Como ocultar atributos do provedor do MDR 750
Como definir os atributos do MDR sem equivalentes do CA CMDB 751
Definir metadados do provedor de dados do CMDBf 751

Capítulo 16: Gerenciando mudanças 753

Gerenciamento de mudanças no CA SDM 753
Componentes do gerenciamento de mudança 754
Exibir o calendário de mudanças 756
Responsabilidades do CAB 756
Como funciona o processo do CAB 757
Atribuir membros ao grupo CAB 757
Responsabilidades do Gerenciador de mudanças 758
Como a função Gerenciador de mudanças funciona 759
Definir tarefas para a função Gerenciador de mudanças 760
Categorias de mudança, status e níveis de risco 761
Exibir o Gerenciador de filas de requisições de mudança 762
Definir uma consulta armazenada de requisição de mudança 762
Configurar opções de Gerenciador de mudanças 764
Calendário de mudança 764
Adicionar informações de cronograma a uma requisição de mudança 765
Modelos de evento do iCalendar 766
Exportar cronogramas para iCalendar 766
Exibições de programação 767
Programando configuração de exibição 769
Como programar requisições de mudança 779

Exemplo de uso do agendador de mudanças ... 780
Como programar janelas de mudança ... 784
Exibir janelas de mudança ... 785
Associar um IC com uma janela de manutenção ... 786
Exibir ICs associados ... 786
Criar um exemplo de janela de blackout ... 787
Criar uma janela de manutenção global ... 788
Análise de conflito e detecção de colisão ... 788
Visualização do CA Workflow ... 789
Como visualizar o fluxo de trabalho ... 789
Change Management Process Definition para o CA Workflow ... 791
Componentes da Change Management Process Definition ... 792
Como configurar a Change Management Process Definition ... 793
Como funciona a Change Management Process Definition ... 799
ActivityNode Actor not found: Update Object -Service Desk r12 ... 813
A requisição de mudança não fecha ... 814
Console do CAB e geração de relatório ... 814
Gerenciar grupos CAB ... 815
Atribuir grupos CAB ... 817
Aprovações do CAB ... 818
Alterar propriedades do Console do CAB ... 818
Geração de relatório de gerenciamento de mudança ... 820
Avaliação de risco ... 821
Como implementar a pesquisa de risco ... 821
Como acessar uma pesquisa de risco diretamente a partir de um URL ... 823
Impact Explorer ... 824
Iniciar o Impact Explorer ... 825
Explorar ICs vinculados ... 825
Exibir um IC no Impact Explorer ... 826
Adicionar um IC relacionado a uma requisição de mudança ... 826
Exibir a Lista de descendentes do IC ... 827
Iniciar o CMDB Visualizer a partir do Impact Explorer ... 827
Configuração do Impact Explorer ... 828

Capítulo 17: Gerenciando relatórios 829

Relatórios do CA Business Intelligence ... 829
Cenários de geração de relatórios ... 830
Componentes de relatórios ... 831

Diagrama do fluxo de dados da geração de relatório 834
Exibir relatórios no InfoView com base na web 835
Segurança e Autorização 836
Grupos e usuários 837
Partição de dados do CA SDM no InfoView 838
Universo e Conexões do Universo 838
Pasta de Relatórios 839
Níveis de Acesso 841
Como apontar um servidor do CA Business Intelligence para um servidor do CA SDM 842
Criar uma origem de dados ODBC 843
Configurar o universo 844
Exportar o universo 844
Como definir a segurança de partições de dados para a geração de relatórios 845
Adicionar o usuário privilegiado do CA SDM ao CMC 845
Definir as credenciais de banco de dados do universo 846
Estabelecer partições de dados 847
Banco de dados replicado para geração de relatórios offline 847
Relatórios de Role-Based 847
Definir relatórios com base na função para a função 848
Exibir novos relatórios na guia Relatórios 850
Relatórios com base na web 857
Interface do BusinessObjects InfoView 858
Navegar para relatórios 858
Preferências do InfoView 859
Relatórios de programação 859
Configuração da análise de dados 860
Publicar e distribuir relatórios 861
Principais indicadores de desempenho 861
Tipos de KPI 861
KPIs predefinidos 862
Daemon do Indicador Principal de Desempenho 862
KPIs de sistema 863
KPIs de consulta armazenadas 865
KPIs SQL 866
Campos KPI 867
Recuperar dados de ticket 868
Solução de problemas 871
Relatórios ad hoc 873

Interface do Web Intelligence 873
Como funciona a geração de relatório ad hoc 874
Exemplo de Relatórios ad hoc 875
Exemplo: Exibir todas as solicitações abertas de prioridade 1 e 2 para todos os usuários 875
Exemplo: exibir todas as solicitações abertas que não incluem um status de trabalho em andamento 877
Exemplo: Exibir todas as solicitações fechadas nos últimos 30 dias por usuários cujos sobrenomes começam com "C" 878
Relatórios do painel 880
Exibir Painéis e Relatórios no InfoView 881
Gravar relatórios do CA Business Intelligence 881
Driver ODBC do CA SDM 882
Escrever SQL para relatórios BusinessObjects 883
Funções do PDM 884
Alias de atributo 887
SQL interativo pdm_isql 887

Capítulo 18: Gerando relatórios no CA SDM 889

Gerar relatórios 889
Exibições de banco de dados 889
Tipo de exibição básico 890
Exibições avançadas 892
Configuração de método de relatório 893
Formatação de relatórios 894
Modificação da ordem de classificação de colunas 895
Relatórios de detalhes e de resumo 895
Relatórios de análise 895
Gerar relatórios de solicitação ou ocorrência 896
Gerar relatórios de área de solicitação ou categoria de ocorrência 896
Gerar relatórios de prioridade de área de solicitação ou de prioridade de categoria de ocorrência 897

Capítulo 19: Gerenciando conhecimento 899

Gerenciamento de conhecimento 899
Localizar procedimentos para gerenciamento de conhecimento 900
Conhecimento e multilocação 900
Como configurar uma base de conhecimento 901
Importar exemplo de dados de conhecimento 902

Monitoramento da base de conhecimento 902
Reindexação da base de conhecimento 902
Configurações de fila de indexação e desindexação para processamento em lote e instantâneo 903
Como usar documentos na base de documentos 904
Envio de conhecimento a partir do CA SDM 906
Envio de conhecimento a partir do Autoatendimento 907
Atributos de documento 907
Permissões do documento 907
Edição de resolução 908
Preparação de publicação de documento 909
Publicação de documento 909
Documentos de versão 909
Expiração de documento 910
Arquivamento e eliminação de documento 911
Pesquisa de conhecimento 911
Fóruns 912
Documentos da árvore de conhecimento 912
Programação de documentos de conhecimento 913
Filtro de cronograma de documento de conhecimento 913
Knowledge Schedule Views 916
Programando configuração de exibição 917
Acessar exportação/importação 924
Como importar/exportar conhecimento 925
Exportar/Importar documentos 928
Exportar/importar pacotes 928
Exibir modelos de exportação/importação 929
Utilitário pdm_ket—Ferramenta de exportação de conhecimento 937
Utilitário pdm_kit—Ferramenta de importação de conhecimento 938
Permitir que usuários exportem e importem conhecimento 939
Web Services 940

Capítulo 20: Administrando o Gerenciamento de conhecimento 941

Administração de conhecimento 941
Localizar procedimentos para administração de conhecimento 942
Funções e papéis do Gerenciamento de conhecimento 942
Interfaces com o usuário do Gerenciamento de conhecimento 944
Funções de configuração e gerenciamento do Gerenciamento de conhecimento 944

Opções de conhecimento de Autoatendimento ... 945
Documentos e usuários ... 952
Como gerenciar os privilégios da função e documentar a visibilidade ... 956
Action Content ... 956
Exibir conteúdo de ação ... 958
Criar conteúdo de ação (URL de ação) ... 959
Crie conteúdos de ação (HTMPL Interno) ... 960
Editar conteúdo de ação ... 961
Pesquisar conteúdo de ação ... 961
Processo de aprovação de documentos ... 962
Gerenciador de processo de aprovação ... 963
Definir um processo de aprovação para a edição de documentos ... 964
Criar um modelo de processo de aprovação ... 965
Definições de status de documento ... 968
Políticas automatizadas ... 970
Exibir políticas automatizadas ... 970
Como configurar políticas automatizadas ... 972
Criar uma política automatizada ... 972
Editar uma política automatizada ... 973
Programar políticas automatizadas ... 974
Exibir relatórios de política de ciclo de vida de documentos ... 974
Controle de documento de conhecimento ... 975
Tipos de comentário ... 976
Modelos de documentos ... 982
Como criar links de documentos de conhecimento ... 990
Categorias de conhecimento ... 993
Criar uma categoria de conhecimento ... 993
Modificar uma categoria ... 997
Excluir uma categoria ... 999
Mover uma categoria ... 1000
Copiar uma categoria com links de documento ... 1000
Copiar uma categoria sem links de documento ... 1001
Gerenciar permissões de categoria ... 1002
Relatórios e métricas ... 1004
Ficha de relatório de conhecimento ... 1005
Relatórios com base na web ... 1006
Formulários da Web de relatórios com base em função ... 1006
Pesquisar ... 1006

Mecanismo de pesquisa do KT ... 1007
Documentos recomendados ... 1020
Defina as opções de pesquisa padrão ... 1025
Opções de integração do CA SDM ... 1026
Definir mapeamento de campo ... 1027
Definir configuração de pesquisa de ocorrências ... 1030
Definir configuração de pesquisa de solicitação/incidente/problema ... 1031
Sugestões de conhecimento ... 1032
Definir categorias de ocorrência ... 1033
Definir as áreas de solicitação/incidente/problema ... 1034
Configurar políticas de Autoatendimento ... 1035
Pesquisa de soluções ... 1036
Definir configurações de perguntas frequentes ... 1037
Definir configurações da pesquisa de soluções ... 1039
Configurações do sistema Gerenciamento de conhecimento ... 1039
Definir configurações gerais ... 1040

Capítulo 21: Administrando o Support Automation 1043

Automatizando o suporte em seu ambiente ... 1043
Assistência online ... 1044
Administração do analista do Support Automation ... 1047
Como os analistas iniciam a assistência online ... 1048
Como configurar a Assistência online para os analistas ... 1049
Como os usuários finais entram em sessões de assistência ... 1050
Como os analistas automatizam o suporte a usuários finais ... 1052
Como os analistas oferecem a assistência online ... 1052
Administração do usuário do Support Automation ... 1053
Como configurar Permissões de função do Support Automation ... 1054
Usuários registrados e anônimos do Support Automation ... 1055
Como configurar o Support Automation para Usuários convidados ... 1055
Administração de nível de acesso do Support Automation ... 1057
Administração de notificação da atividade do Support Automation ... 1058
Adaptações da página do Support Automation ... 1059
Administração de marca ... 1060
Administração de localização ... 1060
Configuração de layout de página ... 1061
Propriedades do sistema Support Automation ... 1062
Administração de fila no Support Automation ... 1062

Gerenciamento de fila....1063
Como gerenciar resumos de fila....1064
Como gerenciar as horas da fila....1065
Gerenciamento de modelo de ticket....1065
Configurações de administração....1066
Como definir as Configurações do Support Automation....1066
Como personalizar as ferramentas do Support Automation....1068
Tarefas automatizadas....1069
Administração de predefinição de bate-papo....1074
Credenciais padrão....1075
Declarações de isenção de responsabilidade....1076
Administração do log da sessão....1076
Exibir o log da sessão....1076
Relatórios do Support Automation....1077
Receber um solicitação de ticket....1079
Convidar o usuário final para uma sessão de assistência....1079
Resolver o ticket com uma sessão de bate-papo....1080
Fornecer assistência online....1081
Encerre a sessão de assistência e feche o ticket....1082

Apêndice A: Exibir descrições de campo 1083

Exibir descrições de campo....1084
View_Act_Log....1084
View_Audit_Assignee....1086
View_Audit_Group....1087
View_Audit_Priority....1087
View_Audit_Status....1088
View_Change_Act_Log....1089
View_Change....1090
View_Change_to_Assets....1096
View_Change_to_Change_Act_Log....1097
View_Change_to_Change_WF....1098
View_Change_to_Properties....1100
View_Contact_Full....1102
View_Contact_to_Environment....1105
View_Group....1106
View_Group_to_Contact....1107
View_Issue....1107

View_Issue_Act_Log ... 1113
View_Issue_to_Assets ... 1114
View_Issue_to_Issue_Act_Log ... 1115
View_Change_to_Request ... 1116
View_Issue_to_Issue_WF ... 1120
View_Issue_to_Properties ... 1123
View_Request ... 1124
View_Request_to_Act_Log ... 1129
View_Request_to_Properties ... 1130

Apêndice B: RFC 2251 Códigos de resultados de LDAP 1133

Códigos de retorno do LDAP ... 1133
Códigos de retorno do servidor LDAP ... 1133
Códigos de retorno do cliente LDAP ... 1139
Padrões de RFC associados ao LDAP ... 1141

Apêndice C: Comandos de referência 1145

bop_sinfo--Exibir informações do sistema ... 1146
dbmonitor_nxd--Daemon de monitoramento de banco de dados ... 1147
pdm_backup--Gravar banco de dados no arquivo ASCII ... 1149
pdm_cache_refresh--Atualizar banco de dados ... 1151
pdm_configure--Abrir a janela de configuração ... 1152
pdm_d_refresh--Start Failed Daemons ... 1153
pdm_deref--Retirar referência dos dados ASCII ... 1154
pdm_discimp -- Importação de ativos descobertos ... 1157
pdm_discupd -- Atualização do ativo descoberto ... 1159
pdm_edit--Configurar processos do servidor ... 1160
pdm_extract--Extrair dados do banco de dados ... 1162
pdm_halt--Terminar daemons ou parar serviços ... 1165
pdm_init--Iniciar daemons ... 1166
pdm_key_refresh--Atualizar informações-chave armazenadas em cache ... 1167
pdm_lexutil--Modificar o léxico do CA SDM ... 1167
pdm_k_reindex — Utilitário de reindexação de documentos de conhecimento ... 1168
    Quando usar pdm_k_reindex ... 1170
    Rastreamento da indexação ... 1170
    Importar e reindexar ... 1171
    Configurações de fila de indexação e desindexação para processamento em lote e instantâneo ... 1171

pdm_listconn--Listar conexões ativas....1172
pdm_load--Adicionar, atualizar e excluir registros do banco de dados 1175
pdm_logfile--Alterar o tamanho de cutover de stdlog....1177
pdm_log4j_config Utility--Modify the log4j properties File 1178
Exemplos de uso do utilitário....1180
Modificar o intervalo de atualização do arquivo de log manualmente 1182
Modificar o appender o jsrvr.log....1183
Modificar o appender o jstd.log....1183
pdm_proctor_init--Iniciar solicitador em servidores secundários 1184
pdm_replace--Substituir uma tabela do banco de dados 1184
pdm_rest_util – Gerenciar o aplicativo serviços web do CA SDM RESTful 1186
Cancela a implantação do aplicativo de serviços web do REST 1186
pdm_restore--Restaurar um banco de dados 1187
pdm_status--Mostrar status de daemons ou processos 1189
pdm_task--Definir variáveis de ambiente 1189
pdm_text_cmd--Interface da linha de comando API do texto 1190
Exemplos de entrada....1192
pdm_uconv--Convert Local Charset to UTF-8....1193
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados 1196
pdm_webstat--Retornar estatísticas de uso da Web 1199
relatório--Gerar relatórios 1203
rpt_srv--Generate Reports....1204
uniconv--Iniciar o daemon conversor de eventos do CA NSM para UNIX....1206

Apêndice D: Grupos de formulários 1209

Grupo de formulários de cliente....1210
Grupo de formulários de funcionário 1211
Grupo Formulários do analista 1213

Apêndice E: Solução de problemas de desempenho 1239

Identificação de problemas de desempenho no CA SDM 1239
Defina o problema de desempenho....1240
Usar a Ferramenta de relatórios de diagnóstico da CA 1241
Executar o script de registro em log do intervalo 1247
Coletar detalhes do ambiente do servidor de banco de dados 1249
Examinar as recomendações gerais de ajuste 1249

Capítulo 1: Introdução

Esta seção contém os seguintes tópicos:

Público-alvo (na página 29)
O que você necessita saber (na página 29)
Processos e práticas recomendadas para gerenciamento de serviços (na página 30)

Público-alvo

Este guia destina-se ao administrado do CA SDM, a pessoa responsável pela administração geral do produto. A seguir estão algumas das tarefas executadas pelo administrador:

- Iniciar e interromper os serviços necessários para o servidor CA SDM.
- Configurar os vários componentes do sistema.
- Determinar as opções disponíveis para usuários.
- Gerar relatórios com base nos dados do Service Desk.

O propósito deste guia é ajudá-lo a usar o CA SDM para implementar, administrar e garantir o fornecimento de serviços. Este guia o ajudará a entender como o produto enfrenta o desafio de automatizar e gerenciar completamente o serviço de fornecimento desde a abertura de uma ocorrência até a sua resolução.

O que você necessita saber

Para administrar o CA SDM com sucesso, você deve estar familiarizado com o seguinte:

- O ambiente operacional no qual o CA SDM está instalado
- A operação de seu servidor web
- Tarefas básicas de administração

Este guia considera que o produto foi instalado com sucesso, com base nas informações do *Guia de Implementação*.

Processos e práticas recomendadas para gerenciamento de serviços

A implementação de processos uniformizados e de práticas recomendadas causa impacto direto na eficácia, produtividade e custo do ambiente de suporte ao serviço. A CA fornece uma biblioteca de processos e práticas recomendados para gerenciamento de serviços, alinhados aos padrões da indústria e estruturas reconhecidas de práticas recomendadas, incluindo ITIL, CobIT, BS15000 e outras. Os processos descritos para o CA SDM incluem:

- Gerenciamento de incidentes
- Gerenciamento de problemas
- Gerenciamento de mudanças
- Gerenciamento de solicitações
- Gerenciamento de configurações
- Gerenciamento de versão
- Gerenciamento de conhecimento
- Support Automation

Observação: informações sobre a biblioteca Melhores práticas estão disponíveis online. Você pode aprender sobre as práticas recomendadas para gerenciamento de serviços da CA, incluindo documentos e outros materiais, em http://www.ca.com/sm/bp http://www.ca.com/sm/bp. Os parceiros especialistas em processos estratégicos da CA podem ajudar a personalizar a biblioteca de práticas recomendadas para sua organização.

Capítulo 2: Gerenciando servidores

Esta seção contém os seguintes tópicos:

Número de servidores (na página 31)
Tarefas de configuração do servidor (na página 32)
Configurando o TCP/IP (na página 33)
Alterar a configuração de um servidor (na página 34)
Configuração do ITIL (na página 34)
Interface PDA (na página 40)
Suporte do Tablet (na página 41)
Interface de usuário móvel de exemplo do REST (na página 42)
Log do Tomcat (na página 55)
Iniciar um servidor secundário (na página 57)
Iniciar o servidor primário (na página 58)
Status do servidor (na página 60)
Configurar SSL no Tomcat (na página 61)
Configurar um servidor secundário do Pintor de telas da web (na página 62)
Como implantar serviços web de CMDBf (na página 63)
Para um servidor (Windows) (na página 63)
Parar um servidor (UNIX) (na página 64)

Número de servidores

Sua instalação do CA SDM tem um ou mais componentes de servidor que você gerencia como administrador. O número de servidores dependerá de sua empresa. Toda instalação possui um servidor principal que gerencia as funcionalidades gerais do CA SDM. Opcionalmente, as instalações podem ter um ou mais servidores secundários a fim de administrar recursos específicos. Após instalar o CA SDM, configure todos os computadores que executam componentes do produto.

Por exemplo, sua configuração específica pode ser um único computador atuando como servidor principal no qual todos os serviços necessários estão instalados. Ou sua instalação pode ser distribuída por vários computadores, cada um com uma função específica. Por exemplo, um computador pode funcionar como servidor primário e servidor de dados, enquanto um servidor web separado executa a interface web e um terceiro computador autentica usuários.

É possível executar a configuração do servidor como parte do processo de instalação, ou executá-la mais tarde. Altere a configuração se ocorrerem mudanças em seu ambiente.

Observação: para obter mais informações sobre a arquitetura deste produto e as opções de configuração, consulte o *Guia de Implementação*.

Mais informações:

Iniciar um servidor secundário (na página 57)
Iniciar o servidor primário (na página 58)

Tarefas de configuração do servidor

Recomendamos que você configure cada computador que está designado para executar o CA SDM. Como administrador, configure o servidor principal; servidor secundário e instalações de clientes. A configuração inicial ocorre como parte do processo de instalação do CA SDM.

Em qualquer ambiente do CA SDM, realize as seguintes tarefas:

- Configurar servidores
- Iniciar, parar e monitorar o servidor principal
- Iniciar, parar e monitorar um servidor secundário (se definido)

Observação: o CA SDM usa o servidor de banco de dados para armazenar e recuperar informações. O servidor de banco de dados é executado como um serviço separado. Para obter informações administrativas, consulte a documentação de seu servidor de banco de dados.

Uma mudança no ambiente do sistema pode exigir alterações na configuração. Por exemplo, é possível modificar a configuração do servidor do CA SDM pelos seguintes motivos:

- Modificações no sistema de gerenciamento de banco de dados
- Modificações feitas no arquivo de modelo de inicialização do CA SDM pelo pdm_edit.pl (um recurso usado para adicionar funcionalidade e aumentar o desempenho do sistema empresarial)
- Integração com um servidor web, como Tomcat
- Integração com o CA EEM

Mais informações:

Iniciar o servidor primário (na página 58)
Para um servidor (Windows) (na página 63)
Parar um servidor (UNIX) (na página 64)
Alterar a configuração de um servidor (na página 34)

Configurando o TCP/IP

É possível modificar a configuração padrão do TCP Internet Protocol (TCP/IP) em um ou mais servidores. Esta definição não pode ser forçada ao cliente se não for suportada no servidor.

A configuração de TCP/IP é controlada usando-se o arquivo NX.env, localizado no diretório $NX_ROOT. Use um editor de texto, como WordPad, para editar este arquivo. A seguinte opção controla a definição de TCP/IP:

NX_PROTOCOL_ONLY=*mode*

em que *mode* pode ser um dos seguintes valores:

IPv4

No modo IPv4, o sistema abre sockets para processos slump que escutam tráfego IPv4.

IPv6

No modo IPv6, o sistema abre sockets para processos slump que escutam tráfego IPv6.

Misto

No modo misto, o sistema abre sockets para processos slump que escutam tráfego IPv4 e IPv6. O modo misto é projetado para clientes com servidores secundários que usam um protocolo de internet diferente daquele do servidor principal (ou entre si).

Observação: se existirem hosts IPv4 e IPv6 na rede, assegure-se de que as estratégias, ferramentas e mecanismos apropriados de transição que suportem essas tecnologias estejam no lugar antes de modificar a configuração do servidor.

Exemplo:

```
NX_PROTOCOL_ONLY=ipv4
```

Alterar a configuração de um servidor

Você pode usar o utilitário de configuração para fazer mudanças em uma configuração do servidor.

Para alterar a configuração de um servidor

1. No menu Iniciar do Windows, selecione Programas, CA, CA SDM, Configuração.

   O utilitário de Configuração do CA SDM é exibido.

2. Preencha os campos do utilitário e clique em Avançar.

   O painel direito muda para mostrar os campos apropriados do link realçado no painel de navegação à esquerda.

3. Continue seguindo as instruções na tela para concluir a instalação e clique em Concluir.

   A configuração do servidor é alterada.

Configuração do ITIL

ITIL (Information Technology Infrastructure Library) é uma coleção de melhores práticas em gerenciamento de centro de dados para computadores. Além de definir processos recomendados, um benefício importante da estrutura de ITIL é a precisão de suas definições da terminologia de centro de dados comumente usada. Frequentemente, no mundo da TI, a mesma palavra é usada com significados diferentes; ou pessoas diferentes usam uma palavra particular com um significado individual. A ITIL ajuda a evitar esse problema.

Os seguintes tipos de ticket estão disponíveis:

- Solicitação
- Requisição de mudança
- Ocorrência
- Incidente
- Problema

Importante: O CA SDM oferece suporte a apenas uma interface ITIL. A interface ITIL oferece suporte a objetos de dados que não eram usados em versões anteriores não ITIL do produto, por exemplo, tickets de problema e incidente.

O ITIL faz o seguinte:

- Produz uma interface ITIL para sua instalação do CA SDM.
- Permite que seu banco de dados, formulários e campos do CA SDM sejam diferentes de uma instalação padrão e estejam em conformidade com as convenções do ITIL.

  Importante: Ao atualizar o sistema existente, desmarque a caixa de seleção Carregar dados padrão para conservar os dados e as tabelas do banco de dados; caso contrário, todos os dados existentes serão perdidos. Para obter mais informações sobre migração de um ambiente diferente do ITIL, consulte o *Guia de Implementação*.

Disciplinas do serviço ITIL

O ITIL descreve melhores práticas para várias disciplinas. As disciplinas de Suporte ao serviço e Fornecimento de serviço combinadas oferecem o recurso de Gerenciamento de serviço a uma organização. Inter-relacionamentos complexos entre todas as dez disciplinas do Gerenciamento de serviços interagem para garantir que a infraestrutura de TI forneça um alto nível de serviço aos negócios.

O Suporte a serviços inclui as seguintes disciplinas:

- Gerenciamento de incidentes
- Gerenciamento de problemas
- Gerenciamento de mudanças
- Gerenciamento de versão
- Gerenciamento de configurações

O CA SDM trata especificamente do Gerenciamento de incidentes, problemas, mudanças e configurações.

O Fornecimento de serviços inclui as seguintes disciplinas:

- Service Management
- Gerenciamento de disponibilidade
- Gerenciamento de capacidade
- Gerenciamento financeiro para Serviços de TI
- Gerenciamento de Continuidade de Serviço de TI

O CA SDM trata especificamente o Gerenciamento de serviços.

Opções de Interface de funcionário e convidado

É possível usar o CA SDM para configurar interfaces separadas para funcionários e convidados. Você configura essas interfaces separadas através do gerenciador de opções na guia administração. Os seguintes valores controlam essas interfaces:

employee_intf_incident_support

Exibe os seguintes valores:

- Somente solicitação
- Somente incidente
- Incidente e solicitação

guest_intf_incident_support

Exibe os seguintes valores:

- Somente solicitação
- Somente incidente
- Incidente e solicitação

Importante: Se esta for uma nova instalação, o ITIL é configurado por padrão com o valor definido como *Somente Incidente*. Se estiver migrando de uma configuração não ITIL anterior, as opções são instaladas, porém os valores são definidos como *Somente Solicitação*.

Configurar a interface de funcionário

Você pode configurar a interface do funcionário para exibir incidentes, solicitações ou ambos.

Para configurar a interface do funcionário

1. Clique na guia Administração.

   O Console de administração aparece.

2. Clique no Gerenciador de opções, Ger. solicitações.

   A página Lista de opções aparece.

3. Clique em employee_intf_incident_support.

   A página Detalhes de opções aparece.

4. Altere o campo Valor da opção para um dos seguintes valores:

   Somente incidente

   (Padrão ITIL) Exibe somente os tipos de ticket de incidente na interface do funcionário.

   Somente solicitação

   Exibe somente os tipos de ticket de solicitação na interface do funcionário.

   Incidente e solicitação

   Exibe tanto os tipos de ticket Incidente quanto Solicitação na interface do funcionário.

   Clique em Salvar.

5. Clique em Atualizar para confirmar suas seleções.

   O Detalhe de opções é atualizado.

6. Feche o Detalhe de opções.

   A página Lista de opções aparece.

Configurar a interface de convidado

Você pode configurar a interface do convidado para exibir incidentes, solicitações ou ambos.

Para configurar a interface do convidado

1. Clique na guia Administração.

   O Console de administração aparece.

2. Clique no Gerenciador de opções, Ger. solicitações.

   A página Lista de opções aparece.

3. Clique em guest_intf_incident_support.

   A página Detalhes de opções aparece.

4. Altere o campo Valor da opção para um dos seguintes valores:

   Somente incidente

   (Padrão) Exibe somente os tipos de ticket de incidente na interface do convidado.

   Somente solicitação

   Exibe somente os tipos de ticket de solicitação na interface do convidado.

   Incidente e solicitação

   Exibe tanto os tipos de ticket Incidente quanto Solicitação na interface do convidado.

   Clique em Salvar.

5. Clique em Atualizar para confirmar suas seleções.

   O Detalhe de opções é atualizado.

6. Feche o Detalhe de opções.

   A página Lista de opções aparece.

Segurança de log de atividade

A opção de segurança de log de atividade impede que usuários finais atualizem um log de atividade. Você pode selecionar a opção interna para evitar que um cliente veja o log.

A segurança de log de atividade afeta logs de atividade dos seguintes tipos de ticket:

- Solicitação
- Requisição de mudança
- Ocorrência
- Incidente
- Problema

Habilitar segurança de log de atividade

Você pode ativar a Segurança de log de atividade a partir do Gerenciador de opções na guia de Administração.

Para ativar a segurança do log de atividade

1. Clique na guia Administração.

   O Console de administração aparece.

2. Clique em Gerenciador de opções, Solicitação-mudança-ocorrência.

   A página Lista de opções aparece.

3. Clique em activity_log_security.

   A página Detalhes de opções aparece.

4. Clique em Editar e selecione um dos seguintes valores de opção:

   Editável

   (Padrão) Permite que todos os campos no log de atividade sejam editáveis através da interface da Web ou serviços web.

   Protegido contra gravação

   Exibe o log de atividade como somente leitura. Se você selecionar a opção interna, somente usuários internos podem editar o log, e ele não poderá ser visualizado pelo cliente.

   Observação: se a opção de segurança estiver ativada, uma mensagem de erro é exibida indicando que o log de atividade é somente leitura se você tentar editar o log através da interface da Web ou origens externas, como serviços web.

   Clique em Salvar.

5. Clique em Atualizar para confirmar suas seleções. Fechar janela

   Segurança de log de atividade está ativada.

Importante: A opção activity_log_security não pode ser instalada. Você somente pode alterar o valor da opção para Editável ou Protegido contra gravação no Gerenciador de opções, Solicitação-mudança-ocorrência.

Impacto no Pintor de tela da Web

O recurso Segurança do log de atividades, $NX_ACTIVITY_LOG_ SECURITY, inclui os seguintes atributos (time_spent, time_stamp e description) para os objetos alg, chgalg e issalg em majic.

Exemplo: $NX_ACTIVITY_LOG_SECURITY para o objeto alg em cm.maj

Neste exemplo, para o objeto alg em cm.maj, $NX_ACTIVITY_LOG_SECURITY aparece em três atributos:

```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL update_cr_timespent(
call_req_id ) 50 ;
 } ;
time_stamp DATE $NX_ACTIVITY_LOG_SECURITY   { ON_NEW DEFAULT NOW ; } ;
description     STRING    $NX_ACTIVITY_LOG_SECURITY;
```

No Web Screen Painter, o campo *Updatable only for new record* é desativado quando o valor da palavra-chave é avaliado como WRITE_NEW.

Observação: para obter informações sobre o Web Screen Painter, consulte o *Guia de Implementação*.

Interface PDA

O CA SDM oferece suporte à terminologia ITIL para a interface do Assistente Digital Pessoal (PDA). Essa interface permite aos usuários finais criar Solicitações, Incidentes e Problemas, bem como pesquisar os seguintes tipos de ticket:

- Incidentes
- Problemas
- Solicitações
- Requisições de mudança
- Ocorrências

Os analistas podem usar a interface do PDA. Essa interface respeita a função presente no campo *Função de PDA* do Tipo de acesso do contato.

Exibe a interface do PDA em todos os navegadores e dispositivos sem suporte.

O serviço de consulta para pesquisar um contato somente funciona nos navegadores de PDA que oferecem suporte a várias guias e várias janelas de navegador. A multilocação funciona de maneira semelhante à interface de navegador, mas a lista suspensa para selecionar a multilocação não é fornecida. Ao criar o ticket, a locação tem por base o solicitante, o usuário final afetado e o analista.

A Calculadora automática de prioridades (APC) ajuda na decisão de prioridade durante a criação de incidentes / problemas, com base em atributos, urgência, impacto, área de solicitação e no usuário final afetado.

Observação: o asterisco indica um campo obrigatório. Por exemplo, quando você cria uma solicitação, especifique o Usuário final afetado e a Prioridade. A interface do PDA não dá suporte a anexos ao criar tickets.

Suporte do Tablet

O Apple iPad exibe a interface de Analista e as interfaces de Autoatendimento para funcionários, Autoatendimento para clientes e Autoatendimento de fornecedores com funcionalidade limitada apenas em seu navegador padrão. O CA SDM não oferece suporte para anexos em Tablets.

Observação: todos os outros Tablets exibem a interface do analista do PDA. No iPad, o navegador Safari oferece suporte para toda a interface de usuário do CA SDM. No entanto, outros navegadores no iPad podem exibir a interface completa do usuário, mas não são suportados.

Interface de usuário móvel de exemplo do REST

A interface de usuário móvel de exemplo do REST fornece duas interfaces de usuário: analista e funcionário. Esse exemplo também oferece suporte às funções de Administrador, Analista de nível 1 e de funcionário. Depois de efetuar logon no CA SDM, as funções de Administrador e de Analista de nível 1 exibem a interface do analista. A função de Funcionário somente exibe a interface do funcionário. Com um logon inválido, o CA SDM, rejeita a solicitação de logon e exibe uma mensagem. Se o administrador tiver desativado o Cálculo automático de prioridade, o campo Prioridade aparece nas páginas de Criar e Editar.

Importante: Esse recurso se aplica somente aos programas de exemplo fornecidos no CA SDM Release 12.7. Ele não é um design restrito no aplicativo de serviços web do REST, propriamente.

Os campos que utilizam sugestão automática exigem um valor seleção da lista de sugestão automática, como o destinatário e Área de incidente. Se você não selecionar um valor, a entrada do usuário para o campo fica vazia.

Observação: recomendamos que você navegue pelas interfaces do REST com os botões fornecidos, em vez de usar as opções de ir para a frente e para trás com o navegador. Por exemplo, selecione Página inicial ou Cancelar para retornar à página anterior.

Configure o REST durante a configuração do CA SDM, mas ative a interface de dispositivo móvel manualmente (na página 46).

Os analistas podem executar as seguintes tarefas:

- Exibir anúncios.

  Padrão: classificado por Data de publicação
- Exibir incidentes que o CA SDM atribuiu ao analista.
- Exibir incidentes atribuídos e não atribuídos.
- Classificar incidentes.

  Padrão: classificado por Data de abertura.
- Pesquisar um incidente.
- Criar um incidente.

- Modificar o status, a urgência e o impacto do incidente.
- Exibir e atualizar o Log de atividades com um comentário ou especificar Retorno de chamada ou Pesquisa.

  Padrão: classificado por Data de atividade.

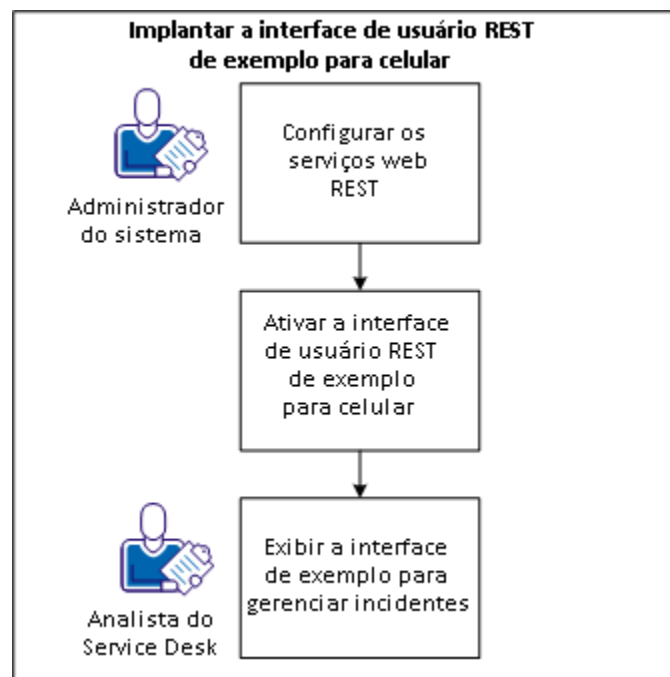
Os funcionários podem executar as seguintes tarefas:

- Exibir anúncios.
- Exibir incidentes abertos e fechados criados por um usuário final.
- Classificar incidentes, como por data de abertura.
- Criar um incidente.
- Atualizar o log de atividade com um comentário.
- Pesquisar um incidente.
- Modificar o status do Incidente de Aberto para Fechado ou de Fechado para Aberto.

Observação: o asterisco indica um campo obrigatório.

Implantar o interface de usuário móvel de exemplo do REST

A interface do usuário móvel de exemplo do REST permite que um Analista do Service Desk gerencie incidentes em dispositivos móveis. O administrador do sistema quer ativar os serviços web do REST e testar o exemplo de interface de usuário móvel. O Administrador do sistema permite os serviços web do REST durante a configuração do produto e copia os arquivos do computador do CA SDM para ativar a interface de usuário móvel de exemplo do REST. O Analista do Service Desk usa a interface de dispositivo móvel para gerenciar incidentes que os usuários finais abram no CA SDM.

O diagrama a seguir explica como um administrador de sistema ativa os serviços web do REST, de modo que um Analista de Service Desk possa gerenciar os incidentes na fila:

1. Configurar os serviços web do REST (na página 45).
2. Ativar a interface de usuário móvel de exemplo do REST (na página 46).
3. Exibir a interface de exemplo para gerenciar incidentes (na página 47).

Configurar os serviços web do REST.

O Administrador do sistema ativa os Serviços web do REST durante a configuração do CA SDM. Por padrão, a configuração do CA SDM não ativa os Serviços web do REST.

Siga estas etapas:

1. Execute *uma* das ações a seguir:
   - Instale o CA SDM e aguarde até que a caixa de diálogo de configuração apareça.
   - Se você já instalou o CA SDM e se ainda não tinha configurado os Serviços web do REST anteriormente, execute o pdm_configure a partir da interface da linha de comando. No Windows, clique em Iniciar, Programas, CA, Service Desk Manager, Configurar.

   A caixa de diálogo Configuração é exibida.
2. Confirme as informações de configuração para Configurações Gerais, Contas do sistema, Banco de dados e Caixas de diálogo da interface web.

   A caixa de diálogo dos Serviços web do REST aparece.
3. Ative a opção Configurar Serviços web do REST.
4. Especifique a Porta do Tomcat do REST.

   Padrão: 8050
5. Especifique a Porta de fechamento do Tomcat do REST.

   Padrão: 8055
6. Clique em Avançar e continue a configuração do CA SDM.

   A configuração está concluída.

Ativar a interface de usuário móvel de exemplo do REST

O CA SDM desativa a interface de usuário móvel de exemplo do REST por padrão para evitar o acesso indesejado ao MDB. O administrador do sistema ativa essa interface manualmente.

Siga estas etapas:

1. Localize o seguinte diretório no computador do CA SDM:

   ```
   $NX_ROOT/samples/sdk/rest/mobiledemo
   ```

2. Copie esse diretório para o seguinte local:

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps
   ```

   Observação: não é necessário reiniciar o Tomcat.

   A interface de usuário móvel de exemplo do REST é ativada.

3. (Opcional) Se você quiser desativar a interface de usuário de exemplo do REST, remova o diretório mobildemo do /webapps.

Exibir a interface pmóvel de exemplo do REST para Gerenciar incidentes.

O Analista do Service Desk vê a interface móvel de exemplo do REST no dispositivo móvel para gerenciar incidentes na fila. Por exemplo, a analista de Service Desk, abre o incidente 30 para registrar um comentário apenas para uso interno.

Siga estas etapas:

1. Abra o seguinte URL no seu dispositivo móvel:

   ```
   http://hostname:REST-Tomcat-port/mobiledemo/login.html
   ```

   A página de logon da interface móvel de exemplo do REST é exibida.

2. Efetue logon no CA SDM usando suas credenciais.

   A página inicial do analista móvel do REST é exibida.

3. Selecione os Incidentes atribuídos.
4. Selecione um incidente, como incidente 30.
5. Selecione Criar atividade na página de detalhes.
6. Selecione Comentário de log na lista suspensa.
7. Selecione Sim na opção interna.
8. Digite um comentário e selecione Salvar.

Você implantou a iInterface de usuário móvel de exemplo do REST com sucesso para que os incidentes possam ser gerenciados na fila.

Ativar a interface de usuário móvel de exemplo do REST

O CA SDM desativa a interface de usuário móvel de exemplo do REST por padrão para evitar o acesso indesejado ao MDB. O administrador do sistema ativa essa interface manualmente.

Siga estas etapas:

1. Localize o seguinte diretório no computador do CA SDM:

   ```
   $NX_ROOT/samples/sdk/rest/mobiledemo
   ```

2. Copie esse diretório para o seguinte local:

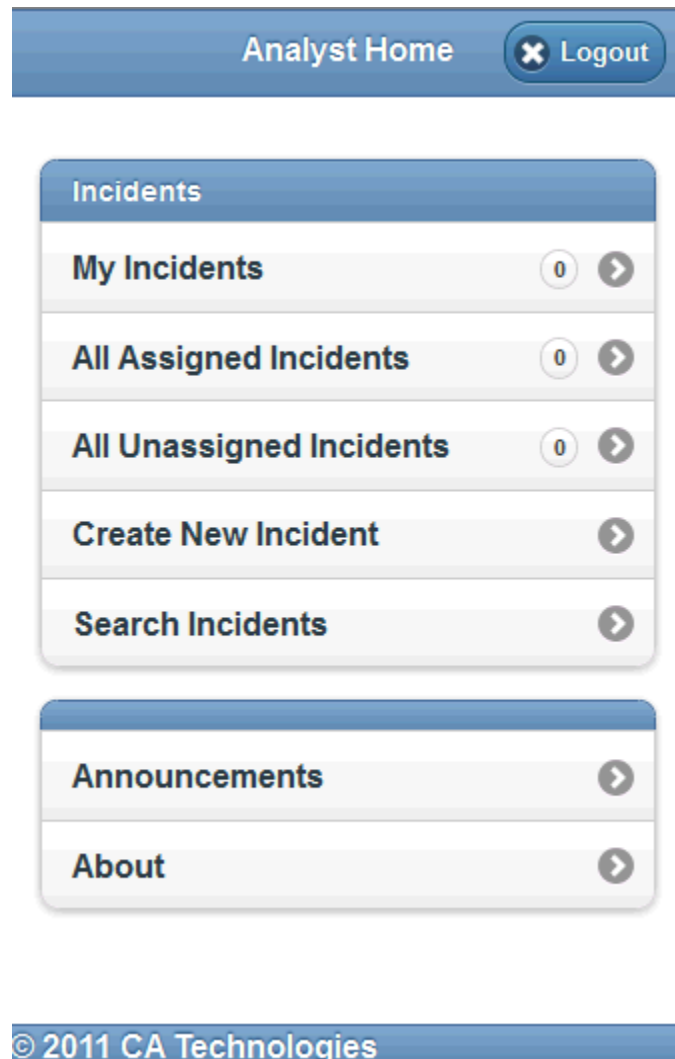
   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps
   ```

   Observação: não é necessário reiniciar o Tomcat.

   A interface de usuário móvel de exemplo do REST é ativada.

3. (Opcional) Se você quiser desativar a interface de usuário de exemplo do REST, remova o diretório mobildemo do /webapps.

Exemplo: página inicial da interface do analista

A imagem a seguir mostra a página inicial do exemplo de analista móvel do REST:

Exemplo: o analista pesquisa um incidente

Nesse exemplo, um analista efetua logon na interface do REST no servidor para procurar o incidente 40.

Siga estas etapas:

1. O analista efetua logon no CA SDM a partir do seguinte URL no dispositivo móvel:

   ```
   http://myservicedesk:8050/mobiledemo/login.html
   ```

   A página inicial do Analista aparece.

2. O analista seleciona Pesquisar incidentes.

   Aparece a página Pesquisa de incidentes.

3. O analista insere os critérios de pesquisa, como o número do Incidente.
4. O analista seleciona Enviar.

   Os resultados da pesquisa de Incidentes são exibidos.

5. O analista seleciona o incidente 40.

   Os detalhes do Incidente de 40 são exibidos.

Exemplo: o analista cria um incidente

Nesse exemplo, um analista efetua logon na interface do REST no servidor. O analista deseja criar um incidente de um problema na rede.

Siga estas etapas:

1. O analista efetua logon na interface móvel do REST.
2. O analista seleciona Criar novo incidente.
3. O analista preenche as seguintes informações:
   - Insere o **Analista** como o usuário final

     Observação: inserir os três primeiros caracteres do nome do usuário abre a lista de sugestão automática. Você pode usar qualquer contato do CA SDM nesse campo.

   - Insere o **ServiceDesk** como o Destinatário
   - Seleciona Abrir na lista suspensa de Status
   - Seleciona a opção 2-Breve na lista suspensa de Urgência

- Seleciona a opção 3-Grupo único na lista suspensa Impacto
- Insere um resumo do incidente

  Por exemplo, o resumo especifica que o analista não pode acessar a rede da empresa em um laptop.
- Insere uma descrição do incidente

  Por exemplo, a descrição especifica o nome do laptop do usuário final na rede e os detalhes de hardware.

4. O analista seleciona Salvar.

   O incidente é criado, e uma mensagem exibe o número do incidente.

Exemplo: o analista registra um Comentário somente para uso interno

Nesse exemplo, um analista abre um incidente para registrar um comentário apenas para uso interno. Os analistas também podem especificar Pesquisar ou de Retorno de chamada do Log de atividades.

Siga estas etapas:

1. O analista efetua logon na interface móvel do REST.
2. O analista completa uma das seguintes etapas:
   - Seleciona Meus incidentes ou Incidentes atribuídos

     Por exemplo, o analista abre um incidente 40 na lista.
   - Seleciona Pesquisar incidentes

     Por exemplo, a analista digita **40** para pesquisar o incidente 40.

   A página de detalhes do Incidente 40 é exibida.
3. O analista seleciona Criar atividade.

   Aparece a página Criar novo log de atividade.
4. O analista seleciona Registrar log na lista suspensa Tipo.

5. O analista seleciona Sim na opção Interna.
6. O analista indica a quantidade de tempo gasto no incidente.

   Observação: se o analista não fornecer um valor para o tempo gasto, o CA SDM exibe a quantidade de tempo entre abrir a página e salvar o log de atividade.
7. O analista insere uma descrição e seleciona Salvar.

   O log de atividade do Incidente 40 é atualizado com um comentário para uso interno apenas.

Exemplo: página inicial da interface do funcionário

A imagem a seguir mostra a página inicial de exemplo de funcionário móvel do REST:

Exemplo: o funcionário cria um incidente

Nesse exemplo, um funcionário efetua logon na interface do REST do servidor para criar um incidente da um problema de rede em seu computador.

Siga estas etapas:

1. O funcionário efetua logon na interface móvel do REST.
2. O funcionário seleciona Criar um novo incidente.
3. O funcionário preenche as seguintes informações:
   - Insere seu número de telefone
   - Insere seu endereço de email
   - (Obrigatório) Seleciona a opção 3-Rapidamente na lista suspensa de Urgência
   - Insere a **Rede** como a Área de incidente
   - Insere um resumo do incidente

     Por exemplo, o resumo especifica que o funcionário não pode acessar a rede da empresa em um laptop.
   - (Obrigatório) Insere uma descrição do incidente

     Por exemplo, a descrição especifica o nome do laptop do usuário final na rede e os detalhes de hardware.
4. O funcionário seleciona Salvar.

   O incidente é criado, e uma mensagem exibe o número do incidente.

Exemplo: o funcionário Edita um incidente

Nesse exemplo, o funcionário deseja editar o incidente 40.

Siga estas etapas:

1. O funcionário efetua logon na interface móvel do REST e seleciona Meus incidentes abertos.

   A página Lista de incidentes aparece.
2. O funcionário seleciona o incidente 40.

   Os detalhes do Incidente de 40 são exibidos.
3. O funcionário seleciona Editar.

4. O funcionário atualiza as seguintes informações sobre o incidente:
   - (Obrigatório) Urgência
   - Área de incidente
   - (Obrigatório) Descrição
5. O funcionário seleciona Salvar.

   O Incidente é modificado.
6. (Opcional) O funcionário seleciona Fechar.

   O incidente é fechado.

Log do Tomcat

O CA SDM usa o arquivo log4j.properties para os componentes da web como o Servlet e PDM_RPC. A Support Automation, o CMDB Visualizer e o REST também têm um arquivo separado: log4j.properties. Iniciar ou interromper o log do Tomcat não requer a reciclagem do dos daemons do Tomcat.

A lista a seguir descreve como os arquivos log4j.properties dos componentes do CA SDM são diferentes:

- O CA SDM monitora as log4j.properties no diretório NX_ROOT\site\cfg e no diretório NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF em busca de mudanças.
- A Support Automation monitora as log4j.properties no diretório NX_ROOT\bopcfg\www\CATALINA_BASE_SA\webapps\SupportAutomation\WEB-INF.
- O CMDB Visualizer monitora o cmdbvisualizerlogging.properties no diretório NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes.
- O REST monitora o rest.log4j.properties no diretório NX_ROOT\site\cfg.

Use o utilitário pdm_log4j_config somente para alterar as variáveis nos arquivos log4j.properties, cmdbvisualizerlogging.properties e rest.log4j.properties. Você não pode usar o utilitário pdm_log4j_config para modificar o intervalo de pesquisa.

O CA SDM verifica os arquivos de propriedades log4j quanto a quaisquer mudanças feitas periodicamente. Configure o intervalo de tempo, modificando a variável NX_LOG4J_REFRESH_INTERVAL no arquivo NX.env.

Padrões do servlet

Os servlets a seguir registram mensagens do nível de INFO no arquivo jsrvr.log, como padrão:

- PDMContextListener: gera uma entrada de log durante a inicialização e o fechamento de serviços.
- PDMweb: gera uma entrada de log das operações na interface do usuário.
- UploadServlet: gera uma entrada de log ao anexar arquivos a um ticket.
- pdmExport: gera uma entrada de log quando o usuário clica em Exportar nos formulários da lista.
- pdm_report: gera uma entrada de log quando você clica no menu Relatório em formulários da lista.
- page_cache: gera uma entrada de log das operações na interface do usuário.
- ProcessServlet: gera uma entrada de log ao instalar o CA Workflow e acessar as tarefas do CA Workflow.

  Observação: o pdm_rpc daemon também gera uma entrada de log a partir dessas ações.
- BOServlet: gera uma entrada de log quando você configurar o CA Business Intelligence e clica na guia Relatórios.

Relatórios do REST

O REST usa os pacotes pdm_rest_util.jar e rest-core.jar que contêm suporte ao log log4j. Esses componentes *não* gravam mensagens nos logs padrão (stdlog.*), mas pelo componente log4j. Por padrão, esses pacotes registram mensagens de INFO, WARN e ERROR. Como os pacotes Java usam o mesmo arquivo de propriedades de configuração do log4j, cada um registra mensagens no mesmo arquivo de saída. É possível exibir o arquivo *rest.log4j.properties* no diretório $NX_ROOT\site\cfg\.

Para aumentar o nível de log a ser rastreado ou depurado, atualize a seguinte seção no arquivo *rest.log4j.properties*:

```
log4j.rootCategory=debug, jrestlog
```

Localize o arquivo de saída, conforme definido no arquivo de propriedades da configuração no seguinte diretório:

```
$NX_ROOT\log\jrest.log
```

Ativar o log CXF

O CA SDM desativa o log CXF por padrão, pois ele pode afetar o desempenho em um ambiente de produção. Se o seu ambiente precisa de log para fins de depuração, o administrador pode modificar o arquivo beans.xml file para ativar o log CXF.

Siga estas etapas:

1. Localize o arquivo beans.xml no seguinte diretório:

   ```
   NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps\caisd-rest\WEB-INF
   ```

2. Localize a seguinte seção do arquivo XML:

   ```
   <cxf:bus>
       <cxf:features>
       </cxf:features>
   </cxf:bus>
   ```

3. Adicione <cxf:logging/> à seção, conforme mostrado no exemplo a seguir:

   ```
   <cxf:bus>
       <cxf:features>
          <cxf:logging/>
       </cxf:features>
   </cxf:bus>
   ```

4. Salve o arquivo XML.

Iniciar um servidor secundário

Se a instalação inclui um ou mais servidores secundários, é preciso iniciar o servidor secundário antes de iniciar o servidor principal.

Em um ambiente UNIX, você inicia cada servidor secundário do CA SDM a partir da linha de comando usando o pdm_proctor_init.

Em um ambiente Windows, você inicia cada servidor secundário do CA SDM usando o servidor Proctor remoto.

Para iniciar um servidor secundário no Windows

1. Selecione Serviços no Painel de controle.

   O Painel de controle é exibido.

2. Selecione o serviço Proctors remotos do CA SDM e clique em Iniciar.

   O serviço é iniciado.

Mais informações:

pdm_proctor_init--Iniciar solicitador em servidores secundários (na página 1184)

Iniciar o servidor primário

Cada instalação do CA SDM tem um servidor principal que gerencia as funcionalidades básicas do produto.

Importante: Se a instalação inclui um ou mais servidores secundários, é preciso iniciar os servidores secundários antes de iniciar o servidor principal.

Para iniciar o servidor primário do CA SDM em um ambiente Windows, no Painel de controle, selecione o serviço do Servidor do CA SDM e clique em Iniciar. Você pode iniciar o serviço manualmente sempre que precisar dele ou pode configurá-lo para iniciar automaticamente como qualquer outro serviço do Windows.

Em um ambiente UNIX, inicie o servidor do CA SDM a partir da linha de comando usando o pdm_init.

A tabela a seguir descreve os processos que iniciam automaticamente ao iniciar o servidor do CA SDM:

Processo	Descrição
Daemon Agent (pdm_proctor_nxd)	O agente daemon responsável por iniciar os daemons gerenciados
Monitor de daemon (pdm_d_mgr)	Monitora os processos de daemon
DB BOP virtual (bpvirtdb_srvr)	Servidor de banco de dados BOP virtual.
Data Dictionary (ddictbuild)	Recria o dicionário de dados sempre que o sistema é iniciado — é executado e desativado
Daemon de KPI (kpi_daemon)	Gerencia a coleta, organização e armazenamento dos dados do KPI.
Oracle agent (orcl_agent)	Agente para o banco de dados Oracle — várias instâncias, de acordo com o carregamento

Processo	Descrição
Oracle DB (orcl_prov_nxd)	Provedor do banco de dados Oracle
Agente SQL (sql_agent) (é executado apenas se você estiver usando o MS SQL)	Agente para banco de dados do SQL Server — muitas instâncias, dependendo do carregamento
SQL DB (sql_prov_nxd) (é executado apenas se você estiver usando o MS SQL)	Provedor do banco de dados do Microsoft SQL Server
Event Manager (ehm_nxd)	Gerenciador de eventos
License Manager (license_nxd)	Gerencia a segurança
Expedidor de mensagem (sslump_nxd)	Envia mensagens
Notification Manager (apenas no Windows) (bpnotify_nxd)	Administra notificações no ambiente Windows
Object Engine (domsrvr)	Servidor CA SDM
Report Manager (pcrpt_nxd)	Relatório de PC
Software Version Control (pdm_ver_nxd)	Administra versões de componentes específicos do sistema
Method Engine (spel_srvr)	Servidor de interpretação de código de verificação ortográfica
Text API (pdm_text_nxd)	Daemon da API de texto para interfaces do CA NSM e email
Timed Events/Notifications (animator_nxd)	Eventos e notificações agendados
User Validation (boplgin)	Logon de Gerenciamento de solicitações
Web Engine (webengine)	Executa o mecanismo do cliente web
Archive Purge Daemon (arcpur_srvr)	Gerencia o processamento em segundo plano do arquivamento e eliminação
BU Daemon (bu_daemon)	Gerencia o cálculo de classificações de pergunta frequente para documentos de conhecimento
DB Monitor (dbmonitor_nxd)	Monitora as mudanças de tabelas comuns da CA
EBR Daemon (bpebr_nxd)	Gerencia solicitações de pesquisa de conhecimento
EBR Idx Daemon (bpeid_nxd)	Gerencia reindexagem do EBR

Processo	Descrição
KRC Daemon (krc_daemon)	Gerencia os cálculos estatísticos e notificações da Ficha de relatório de conhecimento
KT Daemon (kt_daemon)	Gerencia documentos de conhecimento (processo de aprovação, permissões, notificações de documento de conhecimento e assim por diante)
LDAP virtdb (ldap_virtdb)	Agente para comunicação com servidores LDAP
Mail Daemon (pdm_mail_nxd)	Gerencia notificações de email de saída
Mail Eater (pdm_maileater_nxd)	Gerencia notificações de email de entrada
MDB Registration Server (mdb_registration_nxd)	Agente para lidar com solicitações de registro do MDB
PDM KTLC (pdm_ktlc)	Gerencia o licenciamento para o Gerenciamento de conhecimento.
PDM RPC (PDM_RPC)	Gerencia solicitações de Serviços web
Repository Daemon (rep_daemon)	Gerencia repositórios de anexos
Spell checker (lexagent_nxd)	Gerencia as solicitações de verificação ortográfica
Time-to-Violation (ttv_nxd)	Previsor de violações do SLA
tomcat controller (pdm_tomcat_nxd)	Gerencia os serviços do Tomcat

Note: Nesta tabela, o processo do Gerenciador de notificações é pertinente somente ao ambiente Windows, e o processo de banco de dados padrão é pertinente somente ao ambiente UNIX.

Status do servidor

Use o utilitário pdm_status para exibir o status de um servidor primário ou secundário do CA SDM executado em qualquer ambiente operacional.

Mais informações:

pdm_status--Mostrar status de daemons ou processos (na página 1189)

Configurar SSL no Tomcat

É possível configurar o sistema para usar o SSL (Secure Socket Layer) em um servidor web Tomcat.

Para configurar SSL no Tomcat

1. Na linha de comando, altere os diretórios para o local de instalação do JRE e digite o seguinte comando:

   ```
   bin\keytool -genkey -alias tomcat -keyalg RSA
   ```

   Um arquivo .keystore é criado por padrão no diretório principal do usuário que efetuou o logon. Você pode especificar um local diferente durante a criação do arquivo .keystore. No Unix, verifique se o diretório em que você gerar o arquivo .keystore tem permissões suficientes para acessar o CA SDM.

   Observação: para saber mais sobre como especificar um local diferente para o arquivo .keystore, consulte a documentação do Tomcat.

2. Responda os prompts apropriadamente. A senha padrão é *changeit.*

   Observação: você pode inserir uma senha que não a padrão. Para obter mais informações, consulte a documentação do Tomcat.

3. Edite o arquivo server.xml localizado no diretório NX_ROOT\bopcfg\www\CATALINA_BASE\conf, conforme segue:

   ```
   <Connector port="8443" maxHttpHeaderSize="8192"
                  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
                  enableLookups="false" disableUploadTimeout="true"
                  acceptCount="100" scheme="https" secure="true"
                  clientAuth="false" sslProtocol="TLS"
   keystoreFile="keystoreFile="C:\Documents and Settings\user\.keystore"
   keystorePass="password"/>
   ```

4. Use os seguintes comandos para reiniciar o servidor Tomcat:

   ```
   pdm_tomcat_nxd –c stop
   pdm_tomcat_nxd –c start
   ```

5. Para acessar a interface web do CA SDM com SSL, use https://*computer_name*:8443/CAisd/pdmweb.exe. Também é possível produzir o URL dos serviços web de uma maneira parecida.

   Observação: é possível especificar uma porta diferente da 8443 no arquivo server.xml.

6. Exiba e instale o certificado de SSL para acessar o CA SDM.

   O sistema é configurado para usar o SSL (Secure Socket Layer) em um servidor web Tomcat.

7. (Opcional) Se estiver acessando o CA SDM com Internet Explorer, e o Windows Server 2003 estiver configurado para SSL, o navegador exigirá configuração adicional e reinicialização. Em Opções de Internet, guia Avançado, desmarque as seguintes opções na seção Segurança:

   - Verificar revogação de certificados do servidor (requer reinicialização)
   - Não salvar páginas criptografadas em disco

   Depois de reiniciar o navegador, você pode acessar o CA SDM com servidor Tomcat com SSL ativado.

Configurar um servidor secundário do Pintor de telas da web

Se você desejar que um servidor secundário use o Pintor de telas da web, adicione @NX_WSP_CGI_URL ao arquivo nx.env da seguinte maneira:

1. Abra o arquivo the $NX_ROOT/NX.env para edição.
2. Localize a seguinte linha:
   `@NX_WEB_CGI_URL=http://hostname/CAisd/pdmweb.exe`
3. Adicione o seguinte parâmetro após essa linha:
   `@NX_WSP_CGI_URL=http://hostname/CAisd/pdmweb.exe`
4. Salve as mudanças.
5. Recicle os serviços do CA SDM.

   O servidor secundário pode usar o Pintor de telas da web.

Mais informações:

Como modificar o ambiente do sistema (na página 382)

Como implantar serviços web de CMDBf

Após instalar o CA SDM, você pode implementar os serviços web do CMDBf.

Para implementar os serviços web do CA CMDB

1. Verifique se o servidor web está ativo e em execução.
2. Navegue até o diretório CMDBHOME\sdk\websvc\CMDBF.
3. Execute deploy_cmdbws.bat.

   Os serviços web do CMDBf são implementados e iniciados.

Observação: para obter mais informações sobre a implantação dos serviços web do CMDBf, consulte o *Guia de Referência Técnica do CA CMDB*.

Para um servidor (Windows)

É possível parar um servidor CA SDM principal ou secundário em um ambiente Windows.

Para parar um servidor CA SDM em um ambiente Windows

1. Selecione Serviços no Painel de controle.

   A janela Serviços aparece.

2. Selecione o serviço que deseja parar e clique em Parar:

   Servidor CA SDM

   Controla o servidor principal

   Proctor remoto do CA SDM

   Controla um servidor secundário.

   O servidor é parado.

Parar um servidor (UNIX)

É possível parar um servidor CA SDM principal ou secundário em um ambiente UNIX.

Para parar um servidor CA SDM em um ambiente UNIX

1. Feche todos os clientes do CA SDM.
2. Pare o servidor executando o utilitário *pdm_halt*.

   O servidor é parado.

Mais informações:

pdm_halt--Terminar daemons ou parar serviços (na página 1165)

Capítulo 3: Definindo a estrutura comercial

Esta seção contém os seguintes tópicos:

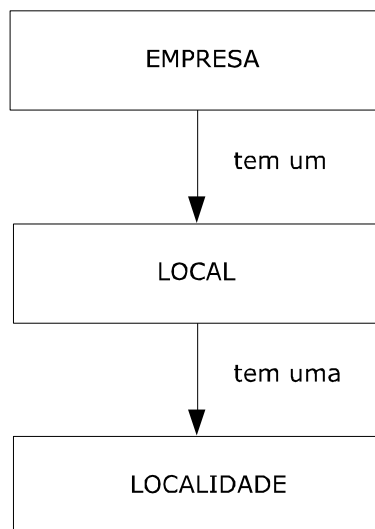
Como definir a estrutura comercial (na página 65)
Definir a infra-estrutura comercial (na página 68)
Multi-locação (na página 72)

Como definir a estrutura comercial

Estrutura comercial é uma representação lógica da organização dentro da qual o CA SDM opera. Para personalizar sua instalação, é possível configurar os objetos de estrutura comercial para melhor atender suas necessidades.

Configure os seguintes objetos para definir a estrutura comercial:

- Sites
- Locais
- Organizações

O diagrama a seguir ilustra o relacionamento entre os objetos na estrutura comercial:

Como uma organização possui (referências) uma localização, que por sua vez possui um local, é necessário definir os objetos na seguinte sequência :

1. Sites
2. Locais
3. Organizações

Dessa maneira, ao definir cada objeto, é possível selecionar dentre objetos existentes em níveis mais baixos na hierarquia.

Observação: para obter informações sobre como definir cada objeto, consulte a *Ajuda online*.

Contatos

Você pode definir cada uma das pessoas que usam o sistema regularmente, como analistas e clientes. Essas pessoas são chamadas de contatos.

Grupos

Um grupo é um conjunto de contatos que representa uma área de responsabilidade específica em seu service desk. Definir grupos permite atribuir a responsabilidade de resolução de tickets quando essa responsabilidade é compartilhada por vários indivíduos.

Por exemplo, você pode ter um grupo de Recursos Humanos em Dallas que é responsável por lidar com ocorrências relacionadas a funcionários no escritório de Dallas de sua organização. Quando um funcionário nesse escritório tiver um problema, você poderá atribuí-lo ao grupo Recursos Humanos em Dallas para obter a resolução.

Você pode associar áreas de solicitação, locais e um turno de trabalho a um grupo que será usado para determinar quando os contatos no grupo poderão aceitar atribuições automáticas de uma solicitação.

Sites

Um *site* é um grupo de locais. Um exemplo de um site seria uma cidade em que sua empresa tem um ou mais locais físicos, ou uma região em que você tem uma base de clientes à qual fornece suporte. Como os locais fazem referência ao site, você deverá definir os sites antes dos locais. Essa seqüência permitirá que você use o novo site no local.

Locais

Locais identificam um local físico específico e permite acompanhar e administrar áreas que se relacionam à sua empresa, como o endereço de uma empresa em particular, uma cidade do endereço do escritório, um prédio ou mesmo um andar de um prédio.

Os locais são os únicos objetos aos quais você pode associar um endereço físico — todos os outros objetos, como organizações, itens de configuração e contatos, derivam seus endereços de seus locais associados.

Você deve definir locais antes de organizações, pois esta sequência permite usar o novo local na organização.

É possível usar locais para atribuir solicitações automaticamente. Para ativar a atribuição automática com base em local, atribua locais a áreas e grupos de solicitação. Os locais de área de solicitação são usados para associar uma solicitação a um local de acordo com o local do item de configuração da solicitação ou do usuário final afetado. Os locais de grupo são então usados para selecionar um grupo ao qual é possível atribuir automaticamente as solicitações nesse local.

Observação: na guia Administração, os tickets são referenciados como áreas de solicitação/incidente/problema. Por questões de brevidade, eles são referenciados aqui como áreas de solicitação.

Organizações

Organizações incluem departamentos internos e divisões ou empresas externas às quais atribuir tickets, classes de itens de configuração e contatos (por exemplo, elas são usadas para identificar a empresa à qual o cliente está associado).

Você pode atribuir a uma organização um tipo de serviço padrão que será automaticamente atribuído aos tickets sempre que essa empresa for especificada. Isso permite associar um nível específico de serviço a um ticket de acordo com a organização atribuída.

Você pode definir itens de configuração para organizações. Definições de itens de configuração permitem especificar hardware, software e serviços que são usados pela organização. Vincular itens de configuração a uma organização (ICs compartilhados) complementa o recurso de vinculação de ICs diretamente a um contato (ICs privados). Quando você designa um contato como o usuário final afetado em uma solicitação, pode então selecionar um IC para a solicitação em listas separadas de ICs privados e compartilhados.

Definir a infra-estrutura comercial

Um aspecto importante da implementação da central de serviços usando o CA SDM é a definição da sua infraestrutura comercial com as configurações dos seguintes objetos:

- Famílias e classes de itens de configuração
- Fabricantes e modelos
- Status de serviço
- Fornecedores e tipos de fornecedor

As seguintes informações fornecem uma descrição geral de cada objeto e explica como ele é usado no produto.

Observação: para obter informações sobre como definir cada objeto, consulte a *Ajuda online*.

Requisição de definição de objetos

Comece pelos níveis inferiores da hierarquia de objeto ao definir objetos. Desta maneira, ao definir objetos em níveis mais altos, você poderá selecioná-los de objetos existentes em níveis inferiores na hierarquia. Por exemplo, como uma classe tem uma família (referências), primeiro é necessário definir as famílias e, em seguida, as classes. Da mesma forma, como os itens de configuração estão no topo da hierarquia, defina-os por último, após definir todos os objetos de suporte. Portanto, defina objetos de dados nas seguintes requisições:

Primeiro a ser definido	Segundo a ser definido	Terceiro a ser definido
Famílias	Classes	Itens de configuração
Fabricantes	Modelos	Itens de configuração
Status de serviço	Itens de configuração	
Tipos de fornecedor	Fornecedores	Itens de configuração

Famílias e classes

Famílias classificam os itens de configuração por tipo e conferem atributos significativos a cada um. *Classes* identificam categorias gerais de itens de configuração suportadas pela sua empresa. Famílias são categorias amplas de itens de configuração, como hardware, software e serviços. Classes são categorias mais específicas dentro da categoria mais ampla de família. Por exemplo, a família hardware pode conter classes como modem, roteador, repetidor e ponte.

Organizar itens de configuração em famílias e classes facilita seu gerenciamento. Por exemplo, é possível gerar uma lista de itens de configuração que pertençam a uma família ou classe específica.

Fabricantes e modelos

Fabricantes identificam os fabricantes dos vários itens de configuração pertinentes à empresa.Os *modelos* contêm informações específicas sobre os produtos que um determinado fabricante fornece a sua empresa. Por exemplo, você pode definir como fabricante uma empresa particular de software. Em seguida, pode definir como modelo cada um dos aplicativos que essa empresa fornece à sua empresa.

Definir fabricantes e modelos facilita o gerenciamento dos itens de configuração. Por exemplo, é possível gerar uma lista de modelos fornecidos por um fabricante específico e também uma lista de itens de configuração de um modelo específico.

Status do serviço

Status de serviço identifica a condição de prontidão de itens de configuração. Exemplos de status de serviço incluem: *em serviço*, *em reparo* ou *descontinuado*. Definir o status de serviço permite acompanhar a disponibilidade e o uso de itens de configuração na empresa. Por exemplo, é possível gerar uma lista de itens de configuração em reparo no momento.

Tipos de fornecedor e fornecedores

Tipos de fornecedor são classificações de fornecedores que identificam o tipo de empresa que fornece os itens de configuração. Por exemplo, é possível classificar fornecedores dos quais você aluga itens de configuração como locadores e classificar fornecedores que prestam serviços como prestadores.

Os *fornecedores* identificam as empresas que fornecem algo à sua empresa, e estabelecem o tipo de empresa e um contato primário. Além de serem consultados por itens de configuração, também é possível consultar um fornecedor no registro de contato de um usuário.

A definição de fornecedores e tipos de fornecedores oferece uma forma conveniente de organizar itens de configuração. Por exemplo, é possível gerar uma lista de fornecedores que se encaixam em um tipo específico de fornecedor e gerar uma lista de itens de configuração de um fornecedor específico.

Itens de configuração

Itens de configuração são os dispositivos, softwares e serviços que formam a infra-estrutura comercial. As informações associadas a um item de configuração identificam exclusivamente o item e indicam sua localização exata. Itens de configuração podem ser associados a contatos (itens de configuração privados) e organizações (itens de configuração compartilhados). Os itens de configuração permitem identificar, exibir e especificar o seguinte:

- Identificar itens de configuração por nome, classe e família.
- Especificar informações de inventário
- Especificar propriedades adicionais para definir o item de configuração.
- Registrar e exibir comentários associados ao item de configuração.
- Especificar informações de localização do item de configuração.
- Especificar informações de serviço, como um tipo de serviço, para o item de configuração.
- Exibir e definir contatos e organizações atribuídos ao item de configuração.
- Identificar relacionamentos hierárquicos e de ponto a ponto entre itens de configuração
- Exibir tickets associados ao item de configuração.

Não é necessário definir todas essas informações para os itens de configuração. No entanto, se você definir uma quantidade ideal de informações do item de configuração, obterá um panorama mais claro quando a análise de impacto for realizada para a organização de TI.

Mais informações:

Criar um item de configuração (na página 543)
ICs Contato, Local e Organização (na página 546)
Relacionamentos do CI (na página 550)

Ferramentas externas de gerenciamento de ativos

É possível integrar sua instalação do CA SDM com outras ferramentas de gerenciamento de ativos, como CA NSM, CA Asset Management e CA APM. Os recursos de gerenciamento de ativos dessas ferramentas do CA SDM incluem o seguinte:

- O CA NSM fornece o utilitário pdm_nsmimp (somente para Windows) para adicionar informações de ativos ao CA SDM.
- O CA Asset Management fornece um conjunto completo de funções de inventário de hardware e software. Ao exibir um IC no cliente do CA SDM, é possível clicar no botão do visualizador de ativos para exibir informações adicionais que foram descobertas sobre o ativo.

  A integração entre o CA SDM e o Unicenter Asset Management é ativada quando os produtos são instalados no mesmo MDB.
- O CA Asset Portfolio Management fornece um conjunto completo de funções de ciclo de vida de ativo. Ao exibir um IC no cliente do CA SDM, é possível clicar no botão do visualizador de ativos para exibir informações financeiras adicionais que foram descobertas sobre o ativo.

  A integração entre o CA SDM e o CA Asset Portfolio Management é ativada quando os produtos são instalados no mesmo MDB.

Observação: para obter mais informações sobre como integrar a instalação do CA SDM com outras ferramentas de gerenciamento de ativos, consulte o *Guia de Implementação*.

Multi-locação

Multilocação é a habilidade de vários inquilinos independentes (e seus usuários) de compartilharem uma única implementação do CA SDM. Usuários inquilinos somente interagem entre si em maneiras definidas, como especificado por suas *funções* e *hierarquias de inquilinos.* Tipicamente, a não ser que os direitos sejam concedidos por uma função ou hierarquia, cada inquilino exibe a implementação do CA SDM somente para seu próprio uso e não pode atualizar ou exibir os dados de outro inquilino.

A multilocação permite que inquilinos compartilhem recursos de suporte a hardware e aplicativos, o que reduz o custo de ambos, ao mesmo tempo em que obtém vários benefícios de uma implementação independente.

Observação: para obter informações sobre como instalar e configurar a multilocação, consulte o *Guia de Implementação*.

Provedor de serviços

O *provedor de serviços* é o inquilino primário (proprietário) em uma instalação de multilocação do CA SDM. O primeiro inquilino adicionado a uma instalação do CA SDM é sempre o inquilino provedor de serviços. O inquilino provedor de serviços não pode ter um inquilino pai.

O CA SDM associa o usuário privilegiado (tipicamente o ServiceDesk no Windows ou srvcdesk no Linux/UNIX) com o inquilino provedor de serviços.

Somente o inquilino provedor de serviços pode realizar qualquer uma das seguintes tarefas do CA SDM:

- Definir opções do CA SDM
- Definir opções do Gerenciamento de conhecimento
- Definir opções do Support Automation
- Criar tabelas ou colunas.
- Criar, editar ou excluir inquilinos
- Permitir que inquilinos tenham subinquilinos
- Atualizar dados públicos

  Observação: um administrador pode conceder usuários inquilinos acesso a dados que não sejam seus próprios. Analistas de inquilinos que não sejam provedores de serviço somente podem ter acesso a seus próprios inquilinos e subinquilinos, a não ser que o acesso de sua função seja atualizado para incluir o inquilino do analista. Por exemplo, a definição de uma função pode definir acessos de leitura e gravação separados para certos grupos de inquilinos para usuários dentro daquela função.

Importante: o primeiro inquilino criado é definido para ser o provedor de serviços, depois disso, a caixa de seleção Provedor de serviços e o campo Status do registro serão somente leitura.

Mais informações:

Administração de provedor de serviços (na página 74)
Acesso do inquilino (na página 77)
Crie um inquilino (na página 90)

Administração de provedor de serviços

O provedor de serviços pode permitir que inquilinos administrem suas próprias configurações. Administradores inquilinos têm acesso a um subconjunto de tarefas de administração que é o mesmo para todos os inquilinos, portanto, a tabela ADMIN_TREE não é ela própria alocada. Ao invés disso, a função Administrador inquilino padrão define as funções de administração que estão disponíveis para administradores inquilinos.

Para designar um usuário como um administrador inquilino, selecione o Administrador inquilino para a função daquele usuário.

Como funciona a Multilocação

Quando a multilocação está ativa, é possível conceder a cada contato acesso a todos os inquilinos (público), um único inquilino ou um grupo de inquilinos (definido pelo usuário ou mantido pelo produto). A função do contato controla o acesso que especifica acesso de leitura e gravação independentemente. Como o acesso de inquilino depende da função e um contato pode alterar funções durante uma sessão, o acesso de inquilino de contato também pode mudar.

Se a multilocação for instalada, a maioria dos objetos do CA SDM inclui um atributo de inquilino que especifica qual inquilino possui o objeto. Os objetos encaixam-se em três grupos, dependendo de seu atributo de inquilino e como ele é usado:

Sem locação

Define objetos sem um atributo de inquilino. Todos os dados nesses objetos são públicos.

Exemplos: Prioridade e urgência.

Inquilino obrigatório

Define objetos com um atributo de inquilino que não pode ser nulo (aplicado pelo CA SDM, não pelo DBMS). Todos os dados nesses objetos são associados a inquilinos individuais; não há nenhum dado público.

Exemplos: tabelas de ticket (Solicitação, Ocorrência e Requisição de mudança).

Inquilino opcional

Define objetos com um atributo de inquilino que não pode ser nulo. Alguns dados nestes objetos são públicos, e alguns estão associados a inquilinos específicos. A exibição do objeto de cada inquilino é uma exibição mesclada dos dados públicos e seus dados de inquilino específico.

Exemplos: categoria e local.

Quando um usuário consulta o banco de dados, o CA SDM restringe os resultados a objetos que pertencem a inquilinos que o usuário está autorizado a acessar. Essa restrição aplica-se além de quaisquer restrições de partição de dados que estejam em vigor. Isso significa que você nunca verá dados em tabelas de inquilinos obrigatórios e inquilinos opcionais, exceto os dados que pertencerem a inquilinos que você tem permissão para acessar.

Quando um usuário de inquilino pede para criar ou atualizar um objeto de banco de dados, o CA SDM verifica se o objeto pertence a um inquilino que a função atual de usuário permite atualizar, e se todas as referências de chave estrangeira (SREL) do objeto a outros objetos são de objetos públicos (sem inquilino), a objetos do mesmo inquilino, objetos provenientes de inquilinos na hierarquia de inquilino acima do inquilino do objeto. Ou seja, um objeto de inquilino tem permissão para fazer referência a objetos que pertencem ao seu inquilino pai, o pai de seu pai, e daí por diante.

Se um usuário que cria um objeto tiver acesso de atualização a vários inquilinos, o usuário deve especificar o inquilino de forma explícita, seja direta ou indiretamente.

Observação: há uma exceção à restrição de referência de SREL. Determinadas referências de SREL (como o destinatário de um incidente) têm permissão para fazer referência a objetos que pertencem a inquilinos na hierarquia de inquilino do objeto contido. Essas referências são designadas como SERVICE_PROVIDER_ELIGIBLE no esquema de objeto do CA SDM (o Majic). O sinalizador SERVICE_PROVIDER_ELIGIBLE faz diferença somente se o inquilino do fornecedor de serviços não estiver na hierarquia de inquilino acima do inquilino do objeto. Se o inquilino do fornecedor de serviços estiver na hierarquia, as regras de validação de inquilino permitem referências de fornecedor de serviços.

Um usuário fornecedor de serviço que pede para criar ou atualizar um objeto está sujeito às mesmas restrições que os usuários de inquilino, exceto pelo fato de que os usuários fornecedores de serviço podem ser autorizados a criar ou atualizar objetos públicos. A função ativa do usuário fornecedor de serviço controla esta autorização.

Observação: se o CA SDM limitar a atualização de dados de inquilino por um usuário, uma mensagem de erro pode anunciar uma limitação de partição de dados. Se você receber essa mensagem de erro, as restrições de partição de dados ou de multilocação entram em vigor.

A opção Multilocação.

Ative a multi-locação instalando uma das seguintes opções de multi-locação:

- **inativo** — A multi-locação não está em uso. Os recursos de multilocação estão indisponíveis, e os objetos não possuem um atributo de inquilino. Esta opção é a configuração padrão em uma nova instalação do CA SDM.
- **configuração**— Os recursos multilocação estão em vigor para administradores, de modo que os objetos e atributos relacionados a inquilino sejam visíveis e editáveis. No entanto, o CA SDM não impõe restrições de locação, e os usuários que não são administradores não visualizam mudanças. Esta configuração permite que um administrador prepare a multilocação, realizando tarefas tais como definir inquilinos ou atribuir objetos a inquilinos sem impactar o uso normal do CA SDM.
- **ativo** — A multi-locação está totalmente operacional. Todos os usuários visualizam as mudanças de UI apropriadas a eles, e o CA SDM impõe restrições de locação.

Observação: para obter mais informações sobre como instalar e implementar a multilocação, incluindo opções adicionais para seu nível de imposição, consulte o *Guia de Implementação*.

Informações do inquilino

Você cria e atualiza inquilinos ao instalar a multilocação (seja na configuração ou no modo de aplicação total). As informações mantidas para um inquilino são similares aos dados mantidos para organização, exceto pelos dois atributos a seguir:

Logotipo

Fornece um URL para um arquivo de imagem com o logotipo do inquilino. O logotipo é exibido tanto na própria página Detalhes do inquilino quanto como um substituto do logotipo da CA em formulários web exibidos por um usuário inquilino ou exibindo um objeto associado ao inquilino.

Provedor de serviços

Indica se o inquilino é o fornecedor de serviços. O inquilino fornecedor de serviços é sempre o primeiro inquilino adicionado. Quando o administrador adiciona o primeiro inquilino, ocorre o seguinte:

- O primeiro inquilino se torna o fornecedor de serviço. Essa designação não pode ser alterada.
- O usuário privilegiado (normalmente ServiceDesk) e todos os contatos de sistema (como System_AHD_Generated) são definidos para pertencer ao novo inquilino provedor de serviços

  Observação: o usuário "Administrador" do sistema é adicionado somente no Windows e é atribuído a um inquilino. O usuário com privilégios deve atribuir manualmente um inquilino ao Administrador.

Acesso do inquilino

A função de um usuário do CA SDM governa a autorização de acesso e a interface do usuário. O conjunto de funções disponíveis para os usuários depende de seu tipo de acesso. A multilocação permite controlar o inquilino ou grupo de inquilinos que um usuário pode acessar dentro da função.

A página de Detalhes da função fornece listas suspensas de Acesso do inquilino e Acesso de gravação do inquilino na guia Autorização. O acesso de inquilino é somente para exibição, e o acesso de gravação do inquilino permite também a criação e a atualização.

É possível atribuir as seguintes associações a funções:

Acesso do inquilino Mesmo que (Somente acesso de gravação do inquilino)

Define o acesso de gravação do inquilino como a mesma configuração do acesso do inquilino. Padrão para acesso de gravação do inquilino e válido somente para acesso de gravação do inquilino.

Todos os inquilinos

Remove restrições de inquilinos. O CA SDM permite que um usuário em uma função com este acesso exiba qualquer objeto no banco de dados (acesso de leitura) ou crie e atualize (acesso de gravação) qualquer objeto alocado no banco de dados. Quando usuários com acesso Todos os inquilinos criam um objeto, o CA SDM requer que eles selecionem o inquilino do novo objeto.

Inquilino único

Define o acesso de inquilino de uma função para um inquilino nomeado. Quando esta opção é selecionada, um segundo campo é exibido na interface web do usuário que permite a seleção de um inquilino específico. O CA SDM restringe um usuário em uma função com este acesso a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com o inquilino nomeado. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Grupo de inquilinos

Define o acesso de inquilino de uma função para um grupo de inquilinos definido pelo usuário ou mantido pelo sistema. Quando a opção Grupo de inquilinos é selecionada, um segundo campo é exibido na interface web do usuário que permite a seleção de um grupo de inquilinos específico. O CA SDM restringe um usuário com a função a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com um dos inquilinos no grupo. Quando um usuário com acesso de grupo de inquilino cria um objeto, o CA SDM exige que selecione o inquilino para o novo objeto. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Inquilino do contato

Define o acesso de inquilino de uma função para o inquilino do contato que o está usando. O CA SDM restringe um usuário em uma função com este acesso a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com seu próprio inquilino. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Grupo de inquilino do contato (somente analistas)

Define o acesso de função de um analista para o grupo de inquilino com o qual o analista trabalha, conforme especificado no registro de contato do inquilino. Se o usuário com a função não for um analista, esta seleção tem o mesmo efeito que Inquilino do contato. É válido tanto para Acesso de inquilino como para Acesso de gravação de inquilino.

Grupo de subinquilinos do contato

Define o acesso de inquilino de uma função para o subinquilino do contato que o está usando. O CA SDM restringe um usuário em uma função com este acesso a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com seu próprio grupo de subinquilino. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Grupo de superinquilinos do contato

Define o acesso de inquilino de uma função para o superinquilino do contato que o está usando. O CA SDM restringe um usuário em uma função com este acesso a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com seu próprio grupo de superinquilino. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Grupo de inquilinos relacionados ao contato

Define o acesso de inquilino de uma função para o grupo de inquilinos relacionados ao contato que o está usando. O CA SDM restringe um usuário em uma função com este acesso a exibir (acesso de leitura) ou criar e atualizar (acesso de gravação) somente aqueles objetos associados com seu próprio grupo de inquilinos relacionados. Esta seleção é válida para Acesso de inquilino ou Acesso de gravação de inquilino.

Todos os usuários podem exibir dados públicos, independentemente dos direitos atuais de acesso de sua função. A caixa de seleção Atualizar público controla se um usuário de provedor de serviços na função tem a autorização para criar ou atualizar dados públicos. Usuários inquilinos (usuários que pertencem a um inquilino diferente do provedor de serviços) não podem atualizar dados públicos, independentemente de sua função.

Mais informações:

Editar um acesso de inquilino para uma função (na página 80)

Editar um acesso de inquilino para uma função

É possível atribuir ou editar acesso de inquilino para uma função.

Para editar um acesso de inquilino para uma função

1. Navegue até Gerenciamento de segurança e das funções, Gerenciamento das funções, Lista de funções.

   A Lista de funções aparece.

2. Clique em uma função.

   A página Detalhes da função aparece.

3. Clique em Editar.

   A página Atualizar função aparece.

4. Selecione opções para um Acesso do inquilino e Acesso de gravação de inquilino.

   Observação: tenha cuidado se selecionar diferentes opções para essas configurações.

5. Clique em Salvar.

   As opções atualizadas de acesso do inquilino são salvas para a função.

Termos de uso de inquilino

Uma instrução de termos de uso apresenta ao usuário final uma instrução de página inicial quando ele efetua logon no CA SDM. A instrução lembra o usuário sobre o uso adequado do produto. O usuário deve concordar com os termos antes que possam continuar a efetuar o logon no CA SDM. As entradas são escritas no log padrão e no log de evento do usuário após a tentativa de logon de sessão.

É possível realizar as seguintes ações de termos de uso:

- Criar, atualizar e excluir uma instrução de termos de uso.
- Associar uma instrução de termos de uso a um inquilino.

  Observação: é necessário ativar a multilocação e configurar um ou mais inquilinos antes de ser possível associar uma instrução de termos de uso a um inquilino.

- Determine que o usuário final aceite a instrução toda vez que efetuar logon.
- Permita que o usuário final ignore a instrução inicial ao apresentar uma instrução de termos de uso em branco.

Mais informações:

Como configurar termos de uso (na página 81)

Como configurar termos de uso

A instrução de termos de uso apresenta ao usuário final uma instrução de página inicial quando ele efetua logon no CA SDM. A instrução lembra o usuário sobre o uso adequado do produto. O usuário deve concordar com os termos antes que possam continuar a efetuar o logon no CA SDM. Se o usuário final selecionar Aceitar, o CA SDM continua com o logon e exibe o formulário principal. Se o usuário selecionar Rejeitar, o CA SDM retorna para o logon. As entradas são escritas no log padrão e no log de evento do usuário após a tentativa de logon de sessão.

Normalmente, você configura a declaração dos termos de uso do inquilino do contato. Se o inquilino do contato não estiver configurado com uma declaração de termos de uso inativa, os termos de uso não estiverem configurados ou se <vazio> for selecionado na lista suspensa Termos de uso, o CA SDM exibe a declaração dos termos de uso para o inquilino pai, avô, e assim por diante. Se nenhuma declaração de termos de uso for encontrada em nenhum nível, o CA SDM procede com o logon. Se você configurar um inquilino com uma declaração de termos de uso em branco, o CA SDM procede com o logon e exibe o formulário principal.

Você pode configurar os termos de uso como segue:

1. Ativar multilocação.
2. Configurar um ou mais inquilinos.
3. Definir uma declaração de termos de uso.
4. Atualizar um inquilino para usar a declaração dos termos de uso.

Observação: para informações detalhadas sobre a criação e a modificação de termos de instruções de uso, consulte a *Ajuda online*.

Impacto na interface com o usuário

Instalar o recurso multilocação modifica a interface com o usuário, dependendo da autorização e do acesso do inquilino associados com a função do usuário. As modificações afetam tanto usuários inquilinos como usuários de provedor de serviços.

Usuários inquilinos

Se a função de um usuário é restrita a um único inquilino e o usuário não é um administrador, é possível substituir um logotipo personalizado de inquilino pelo logotipo padrão da CA Technologies em todas as páginas. Esta substituição depende se o logotipo é definido na página de Detalhe do inquilino e, portanto, é opcional para o inquilino.

A única mudança na interface do usuário para usuários inquilinos não administradores é que os itens ou botões de menu que permitem atualização ou edição (o botão Editar ou o botão Criar novo em uma página de lista) são suprimidos para objetos públicos, porque usuários inquilinos não são autorizados a atualizar um objeto público.

Administradores inquilinos

Administradores de inquilinos com acesso para Inquilino único que exibam objetos com inquilino opcional veem uma mudança adicional na interface. Páginas de lista para estes objetos incluem uma coluna Público especificando se a linha de lista é dados públicos. Adicionalmente, o primeiro elemento no filtro de pesquisa é uma lista suspensa de Dados públicos contendo as seguintes seleções:

- Incluir (padrão)
- Excluir
- Somente

Um administrador de inquilinos com acesso a vários inquilinos vê uma coluna Inquilino em páginas de lista para qualquer objeto com locação. Esta coluna toma o lugar da coluna Público em listas de tabelas com inquilino opcional.

Usuários que podem exibir um grupo de inquilinos

Se a função de um usuário permitir acesso de exibição para vários inquilinos, ou um usuário de provedor de serviços tiver autorização Atualizar público, os formulários de lista do CA SDM modificarão da seguinte forma:

Objetos sem inquilino

Objetos sem inquilino contêm apenas dados públicos. Um usuário de provedor de serviços tem permissão de criar ou atualizar um objeto sem locação somente se sua função tiver autorização Atualizar público. Se não, a interface do usuário suprime itens ou botões de menu que permitem atualização ou edição, como o próprio botão Editar, ou o botão Criar novo em uma página de lista. Usuários inquilinos não podem atualizar objetos públicos, e esses usuários nunca veem um botão Editar ou Criar novo em uma página de lista para um objeto sem locação.

Objetos com inquilino obrigatório

Objetos de inquilino obrigatório contêm apenas dados relacionados a um inquilino específico. Formulários de lista para esses objetos automaticamente incluem uma coluna Inquilino depois da última coluna de link. Adicionalmente, o filtro de pesquisa contém um seletor de inquilino permitindo que o usuário restrinja a lista a um único inquilino.

Objetos de inquilino opcional

Os objetos de inquilino opcional contêm tanto dados públicos como específicos do inquilino. Formulários de lista para esses objetos automaticamente incluem uma coluna Inquilino (um inquilino em branco indica um objeto público). Adicionalmente, o filtro de pesquisa contém um seletor de inquilinos e uma lista suspensa de Dados públicos (a mesma visualização por administradores de inquilinos).

Observação: se tabelas que requerem inquilinos incorretamente contiverem dados sem locação em um sistema de multilocação, uma lista suspensa de dados públicos será exibida nestas tabelas e a seguinte mensagem é exibida: “AHD05358 There were nn untenanted active xxx objects at Service Desk startup.”

Usuários que podem atualizar vários inquilinos

Se a função do usuário permite acesso a vários inquilinos, ou a função do usuário de um provedor de serviços tem autorização Atualizar público (típico para um analista que trabalha para um provedor de serviços), as páginas de detalhe mudam conforme segue:

Objetos sem inquilino

Objetos sem inquilino contêm apenas dados públicos. Não existem modificações nas páginas de detalhe para um usuário de provedor de serviços com autorização Atualizar público. Se o usuário estiver em uma função sem autorização Atualizar público, ou não pertencer ao provedor de serviços, páginas somente leitura para objetos sem locação não terão um botão Editar.

Objetos existentes com inquilino obrigatório

Objetos de inquilino obrigatório contêm apenas dados relacionados a um inquilino específico. Páginas de detalhe para objetos existentes com inquilino obrigatório exibem o inquilino do objeto como parte do cabeçalho padrão da página.

Objetos de inquilino opcional

Os objetos de inquilino opcional contêm tanto dados públicos como específicos do inquilino. A página de detalhe para esses objetos depende de o usuário pertencer ao provedor de serviços e estar em uma função com autorização Atualizar público:

- Se a função do usuário de um provedor de serviços tiver autorização Atualizar público, a página de detalhe será a mesma que aquela para objetos obrigatórios para inquilinos.
- Se a função do usuário não tiver autorização Atualizar público, ou se o usuário não pertencer ao provedor de serviços, páginas de detalhe para objetos públicos não terão um botão Edição.. Outras páginas de detalhe são as mesmas que aquelas de objetos com inquilino obrigatório.

Impacto no Support Automation

O impacto de multilocação em seu ambiente de suporte depende de restrições de inquilinos e funções colocadas em usuários finais e analistas. O Provedor de serviços gerencia permissões de leitura/gravação tanto para dados públicos como pra dados específicos de inquilinos. Por exemplo, um analista pode processar sessões de assistência a partir da fila pública e de uma fila específica de inquilinos, mas o analista só pode usar ferramentas de Assistência online ativadas para cada inquilino.

Para usuários finais com acesso ao Support Automation, não configure o usuário final para ter acesso de gravação a um inquilino que não seja um subinquilino do inquilino proprietário do usuário final, a não ser que o grupo da chave estrangeira (FK) seja alterado para incluir o inquilino proprietário. Se o usuário final selecionar um inquilino para logon, ou for convidado através de um ticket para um inquilino que não atenda a este critério, receberá uma mensagem de erro ao tentar acessar o cliente de usuário final do Support Automation. Esta restrição não se aplica se o inquilino proprietário do usuário final for o inquilino provedor de serviços.

Para analistas com acesso ao Support Automation, não configure o analista para ter acesso de gravação a um inquilino que não seja um subinquilino do inquilino proprietário do analista, a não ser que o grupo da chave estrangeira (FK) seja alterado para incluir o inquilino proprietário. Se o analista tentar processar um usuário final, ou convidar um usuário final a partir de um ticket, em um inquilino que não atenda a estes critérios, o analista receberá um erro.

Analistas e usuários finais sem acesso de leitura a seu inquilino não podem iniciar o cliente do Support Automation. Para analistas, uma mensagem de aviso é exibida no CA SDM neste caso, como a partir da guia principal do Support Automation.

É possível usar as seguintes funções para gerenciar usuários do Support Automation:

Analista da Support Automation

Fornece suporte ao usuário final usando a Assistência online. O Provedor de serviços determina o acesso de inquilino apropriado e pode ativar as ferramentas de Assistência online e acesso de leitura/gravação para tarefas automatizadas.

Importante: Se um analista que não é de Provedor de serviços tem direito de leitura a um inquilino pai, filho ou não relacionado, o acesso à função deve ser atualizado para aquele inquilino. Os analistas que não possuem acesso de leitura a seu inquilino não podem executar o cliente de analista do Support Automation, e uma mensagem de aviso é exibida no CA SDM, tal como da guia Support Automation principal ou de um ticket.

Administrador de Support Automation

Configura o ambiente do Support Automation para analistas e usuários finais. O Provedor de serviços determina seu acesso de inquilino e permite que você exiba uma lista suspensa de inquilinos em formulários de Lista e Detalhes. Esses formulários permitem selecionar inquilinos ou dados públicos específicos durante a pesquisa, criação e modificação de dados do Support Automation em um ambiente de multilocação.

Observação: objetos como filas, níveis de privacidade e predefinições de bate-papo são opcionais para o inquilino.

Impacto do Gerenciamento de conhecimento

O impacto de multilocação em seu ambiente de conhecimento depende das restrições de inquilino que foram colocadas nos usuários:

Usuários inquilinos

Substitui o logotipo do inquilino padrão se a função for restrita a um único inquilino.

Administradores inquilinos

Permite que os administradores exibam dados públicos e específicos de inquilino. Páginas de lista para estes objetos incluem uma coluna Público especificando se a linha de lista é pública.

Ao pesquisar por conhecimento, o filtro contém uma lista suspensa de Dados públicos com seleções de Incluir (padrão), Excluir e Somente.

Observação: objetos como modelos de processo de aprovação, categorias, documentos, arquivos e fóruns são opcionais para o inquilino.

Categorias e documentos de conhecimento

Ambos os documentos de conhecimento e categorias de conhecimento são opcionais do inquilino. Considere as seguintes informações para objetos opcionais e públicos de inquilino:

- Os documentos de conhecimento público somente podem ser adicionados nas categorias de conhecimento público.
- As categorias de conhecimento público somente podem ser adicionadas nas categorias públicas.
- As categorias de inquilinos podem ser adicionadas em categorias públicas e em categorias de inquilino.
- Apenas os documentos de inquilino podem ser adicionados em categorias de inquilinos.
- Os documentos públicos e de inquilinos podem ser adicionados em categorias públicas.

Observação: A funcionalidade da categoria Recortar/Copiar/Colar é permitida apenas se a origem e o destino tiverem o mesmo inquilino, ou se o destino for público.

Os repositórios são definidos como opcional de inquilino, portanto, o administrador pode criar repositórios diferentes para inquilinos diferentes.

As imagens incluídas são permitidas apenas quando o documento e a imagem estão definidos para o mesmo inquilino. As pastas de anexo, anexos e anexos para links de documento também estão definidos como opcional de inquilino.

Classificação da pergunta freqüente

Ao visualizar a classificação das perguntas frequentes para usuários inquilinos, considere as seguintes informações sobre documentos públicos:

- Os documentos públicos são visualizados por uma audiência maior do que os usuários inquilinos.

  A classificação das perguntas frequentes de documentos públicos é maior do que a de documentos específicos de um inquilino.
- Cada inquilino possui necessidades diferentes, portanto, os padrões de uso são diferentes entre inquilinos.

As principais soluções na página inicial de autoatendimento do CA SDM exibe os cinco documentos públicos principais, bem como os cinco documentos principais de um inquilino.

É possível configurar as principais soluções, navegando até o conhecimento, pesquisa de soluções, configurações de perguntas frequentes na guia Administração.

Ficha de relatório de conhecimento

A ficha de relatório de conhecimento permite que os analistas e administradores visualizem diversas métricas, tais como criação de documentos, publicação, localizações e votos. Este relatório é para um período de tempo predeterminado, por analista, categoria e organização.

Ao usar a ficha de relatório de conhecimento para fornecer informações para uma função que possui acesso de inquilino único, os dados são limitados pelos critérios do inquilino.

Como usar a Multilocação

Use os seguintes procedimentos para administrar os recursos de multilocação do CA SDM

Exibir inquilinos

É possível exibir inquilinos a partir de qualquer Lista de inquilinos.

Observação: esse recurso está disponível somente se multilocação estiver instalado (no modo ligado ou de configuração);

Para exibir um inquilino

1. Na guia Administração, selecione Gerenciamento da segurança e das funções.
2. Clique em Inquilinos.

   A Lista de inquilinos aparece.
3. (Opcional) Selecione um inquilino na Lista de inquilinos.

   A página Detalhes do inquilino aparece.

Observação: listas de inquilinos também são exibidas nas páginas como Detalhes do grupo de inquilinos e Inquilinos afetados pelo IC.

Crie um inquilino

Você pode usar o produto para criar um inquilino.

Para criar um inquilino

1. Selecione Gerenciamento da segurança e das funções, Inquilinos na guia Administração.

   A página Lista de inquilinos aparece.

   Observação: a opção Gerenciamento de segurança e função, Inquilinos está disponível quando o recurso de multilocação está instalado (no modo ligado ou de configuração).

2. Clique em Criar novo.

   A página Criar novo inquilino é exibida.

3. Complete os campos editáveis, se necessário:

   Nome

   Exibe o nome do inquilino.

   Provedor de serviços

   Identifica se um inquilino é o fornecedor de serviços. O primeiro inquilino criado é sempre o Provedor de serviços.

   Número do inquilino

   (Informações somente) Exibe o número do inquilino. Esse campo não é usado pelo CA SDM.

   Status do registro

   Define o inquilino como Ativo ou Inativo.

   Inquilino pai

   Especifica o inquilino acima deste inquilino, tornando esse inquilino um *subinquilino* em uma hierarquia de inquilino.

   Subinquilinos permitidos

   Permite que esse inquilino tenha subinquilinos. O inquilino não pode modificar a configuração.

   Profundidade do inquilino

   (Apenas informação) Indica a profundidade de inquilino deste inquilino.

Grupo de superinquilinos

(Apenas informação) Identifica o grupo de inquilino mantido pelo sistema que contém esse inquilino e todos os inquilinos acima dele na hierarquia de inquilinos.

Grupo de subinquilinos

(Apenas informação) Identifica o grupo de inquilino mantido pelo sistema que contém esse inquilino e todos os inquilinos abaixo dele na hierarquia de inquilinos.

Grupo de chaves estrangeiras

(Apenas informação) Identifica o grupo de inquilinos mantido pelo sistema que contém inquilinos que podem ser referidos a partir de um SREL em dados que pertencem a esse inquilino. O grupo de chave estrangeira é o mesmo que o grupo de superinquilino.

Grupo de inquilinos relacionados

(Apenas informação) Identifica o grupo de inquilinos mantido pelo sistema que consiste tanto no grupo de superinquilinos quanto no de subinquilinos para esse inquilino.

Termos de Uso

Especifica a instrução de Termos de uso para o inquilino.

Logotipo

Especifica o URL para o arquivo de logotipo do inquilino, que pode ser qualquer tipo de imagem da web.

Local

Exibe a página de Pesquisa de local.

Contato

Exibe a página Pesquisa de contato.

Observação: se nenhum contato estiver associado ao inquilino correspondente, os campos Endereço de email e Endereço de email do pager estão inativos.

4. Clique em Salvar.

   O Inquilino é criado.

5. Feche a janela.
6. Clique com o botão direito do mouse na lista Inquilino e clique em Atualizar.

   A Lista de inquilinos é atualizada e exibe o inquilino criado.
7. (Opcional) Para atribuir esse inquilino a grupos de inquilino definidos pelo usuário, clique em Atualizar grupos de inquilinos na guia Grupos de inquilinos.

Editar um inquilino

Você pode editar um inquilino na guia Administração.

Observação: esse recurso está disponível somente se multilocação estiver instalado (no modo ligado ou de configuração);

Para editar um inquilino

1. Na guia Administração, selecione Gerenciamento da segurança e das funções.
2. Clique em Inquilinos.

   A Lista de inquilinos aparece.
3. Clique com o botão direito do mouse em um inquilino e clique em Editar.

   A página Atualizar inquilinos aparece.

   Observação: ao editar um inquilino existente, as guias Subinquilinos e Itens de configuração são exibidas.
4. Faça as mudanças necessárias e clique em Salvar.
5. Feche a página Atualizar inquilino.

   A Lista de inquilinos aparece.
6. Clique com o botão direito do mouse e selecione Atualizar.

   A Lista de inquilinos atualizada é exibida.

Hierarquias de inquilinos

Uma *hierarquia de inquilino* é um grupo de inquilino estruturado que é criado ou modificado pelo sistema quando você atribui um *inquilino pai* a um inquilino. O inquilino torna-se um *subinquilino* do pai e dos inquilinos superiores (se houver) nessa hierarquia.

Observação: O provedor de serviços pode criar várias hierarquias não relacionadas, ou nenhuma. Mesmo em um sistema com hierarquias de inquilino, é possível definir inquilinos independentes.

Um subinquilino geralmente representa uma subdivisão dentro de seus *superinquilinos*. Um subinquilino pode ter suas próprias regras e dados de negócios, e dados de superinquilino são automaticamente enviados ao subinquilino somente para leitura.

O CA SDM oferece uma hierarquia de inquilino de profundidade ilimitada. No entanto, o *provedor de serviços* pode especificar um limite sobre o número total de inquilinos e a profundidade de hierarquias de inquilino (o padrão é quatro níveis). O provedor de serviços também determina se inquilinos individuais podem ter subinquilinos.

Observação: O provedor de serviços pode fazer parte de hierarquias de inquilino, porém isso não é obrigatório. O provedor de serviços não pode ter um inquilino pai.

Criar um subinquilino

O sistema de subinquilinos permite criar e modificar hierarquias de inquilinos para fins organizacionais e de compartilhamento de dados. Para colocar um inquilino em uma hierarquia de subinquilino, você atribui um inquilino pai a ele.

Para criar um subinquilino

1. Na guia Administração, selecione Gerenciamento de segurança e função, Inquilinos.

   A Lista de inquilinos aparece.

   Observação: a opção Gerenciamento de segurança e função, Inquilinos está disponível somente quando recurso de multilocação está ativado.

2. Clique em um inquilino existente para Editar ou clique em Criar novo.

   A página Detalhes do inquilino aparece. Insira quaisquer dados ou mudanças.

3. Selecione um inquilino pai.

   Observação: a lista suspensa Inquilino pai somente exibe inquilinos que têm permissão para ter subinquilinos.

4. Clique em Salvar.

   O inquilino é um subinquilino do inquilino pai.

   Observação: quando um inquilino é um subinquilino, ele pertence ao grupo Subinquilino do inquilino pai, assim como os subinquilinos (se houver) desse subinquilino, e assim por diante. O inquilino pai faz parte do grupo Superinquilino do inquilino, assim como os superinquilinos (se houver) desse superinquilino, e assim por diante. Cada um faz parte do grupo Inquilinos relacionados do outro.

Grupos de inquilino mantidos pelo sistema

O CA SDM gera e mantém os três grupos de inquilino automaticamente para cada inquilino em uma hierarquia de inquilino (*inquilino* é o nome do inquilino):

- *tenant*_subtenants (inquilino, seus inquilinos filhos, e seus subinquilinos inferiores)
- *tenant*_supertenants (inquilino, seu inquilino pai e seus superinquilinos superiores)
- *tenant*_relatedtenants (toda hierarquia única)

Os grupos de inquilino mantidos pelo sistema podem ser usados como grupos de inquilino definidos pelo usuário. Entretanto, somente seus nomes e descrições podem ser modificados.

Exibir grupos de inquilinos

Você pode ver as informações do grupo de inquilinos para mostrar integrantes do grupo.

Observação: esse recurso está disponível somente se multilocação estiver instalado (no modo ligado ou de configuração);

Para visualizar a lista de grupo de inquilinos.

1. Na guia Administração, selecione Gerenciamento da segurança e das funções.

2. Clique em Grupos de inquilinos.

   A Lista de grupos de inquilinos aparece.

   Observações: você pode selecionar exibir ou ocultar grupos de inquilinos mantidos pelo sistema.

3. (Opcional) Selecione um Grupo de inquilinos na lista.

   As informações do grupo de inquilinos são exibidas.

4. Modifique o grupo de inquilinos se necessário.

Criar um grupo de inquilinos

Você pode usar o produto para criar um grupo de inquilinos.

Para criar um grupo de inquilinos

1. Na guia Administração, selecione Gerenciamento da segurança e das funções.

2. Clique em Grupos de inquilinos.

   A Lista de grupos de inquilinos aparece.

   Observação: a opção Gerenciamento de segurança e função, Grupos de inquilinos está disponível somente quando o recurso de multilocação está instalado (no modo ligado ou de configuração).

3. Clique em Criar novo.

   A página Criar novo grupo de inquilinos aparece.

4. Preencha os seguintes campos:

   Nome do grupo de inquilinos

   Exibe o nome do grupo de inquilinos.

   Status do registro

   Define o grupo de inquilinos como ativo ou inativo.

   Descrição

   Exibe uma descrição do grupo de inquilinos.

5. Clique em Salvar.

   O grupo Inquilino é criado.

6. Feche a janela.

   A Lista de grupos de inquilinos aparece.

7. Clique com o botão direito do mouse na lista Inquilino e selecione Atualizar.

   A Lista de grupo de inquilinos é atualizada.

8. Clique em Atualizar inquilinos na página Detalhes do grupo de inquilinos para adicionar integrantes inquilinos ao grupo.

Editar um grupo de inquilinos

Você pode editar um grupo de inquilinos para gerenciar seus integrantes e informações detalhes.

Observação: esse recurso está disponível somente se multilocação estiver instalado (no modo ligado ou de configuração);

Para editar um grupo de inquilinos

1. Na guia Administração, selecione Gerenciamento da segurança e das funções.
2. Clique em Grupos de inquilinos.

   A Lista de grupos de inquilinos aparece.

3. Clique com o botão direito do mouse em um grupo de inquilinos e clique em Editar.

   A página Atualizar grupo de inquilinos é exibida.

4. Faça as mudanças necessárias e clique em Salvar.
5. Feche a janela.

   A Lista de grupos de inquilinos aparece.

6. Clique com o botão direito do mouse na janela e selecione Atualizar.

   A Lista grupo de inquilinos atualizada é exibida.

Atribuições de dados do inquilino

O CA SDM exibe o inquilino no mesmo formato nas versões Exibir e Editar de uma página de detalhe para um objeto existente, porque o inquilino para um objeto existente não pode ser modificado a partir da interface da Web.

Ao editar um objeto com locação, listas suspensas na página de edição são automaticamente restritas a valores que sejam públicos, de propriedade do mesmo inquilino que o objeto base, quaisquer inquilinos acima da hierarquia do inquilino ou de propriedade do provedor de serviços (se a lista suspensa aplicar-se a um atributo SERVICE_PROVIDER_ELIGIBLE).

Não existem modificações na página de detalhe para objetos de pesquisa associados com um objeto com locação. Se um usuário com acesso a vários inquilinos clicar em um link de pesquisa para uma tabela alocada, o mecanismo da web automaticamente restringirá a pesquisa a valores apropriados para o atributo e exibirá uma mensagem de faixa no formulário de lista ou pesquisa pop-up.

Observação: restrições de inquilino não são exibidas no filtro de pesquisa e não podem ser modificados pelo usuário.

O inquilino torna-se um seletor (uma lista de pesquisa ou suspensa) quando você cria um objeto com inquilino obrigatório.

Se o campo inquilino estiver vazio, é possível especificar um valor de inquilino diretamente preenchendo o campo, ou indiretamente especificando um valor para um atributo que implica um inquilino (como Usuário final afetado). A interface exibe os seguintes sufixos:

(T)

Indica um atributo que implica um inquilino, que é uma pesquisa para uma tabela com inquilino obrigatório.

(TO)

Indica um atributo que opcionalmente implica um inquilino, ou seja, uma pesquisa para uma tabela com inquilino opcional.

As propriedades de web.cfg controlam o texto desses indicadores.

Exceto pelo atributo inquilino em si, atributos que implicam inquilino são sempre exibidos como pesquisas, mesmo se criados com uma macro dtlDropdown.

O CA SDM automaticamente define o inquilino ao pesquisar ou preencher automaticamente um valor alocado em qualquer campo que implica inquilino (exceto que, preencher um campo SERVICE_PROVIDER_ELIGIBLE com uma referência a um objeto provedor de serviço, não define o inquilino). Após a definição do inquilino, as pesquisas de campos relativas a inquilino são restritas da mesma forma que as pesquisas de objetos alocados existentes.

Observação: até que o objeto seja salvo, o campo inquilino permanece editável, e é possível modificar o inquilino atualizando-o diretamente. Ao modificar o inquilino, o CA SDM automaticamente limpa campos que implicam inquilino contendo referências a objetos que pertençam ao inquilino anterior.

O CA SDM normalmente inicia o selecionador de inquilino como vazio. É possível modificar este comportamento de várias formas:

- Abra a página Criar novo a partir de uma página como Perfil resumido, que preenche previamente um campo que implica inquilino
- Defina a preferência de usuário Reter inquilino

  Esta é uma nova preferência de usuário que inicializa o inquilino para novos objetos com o mesmo inquilino que a última página visualizada ou atualizada, ou na última restrição de filtro de pesquisa de página de lista.
- Abra a página com um URL que explicitamente especifique um inquilino

  Isto não é fornecido em nenhum URL predefinido, mas está disponível para permitir que locais criem itens ou botões de menu que especifiquem um inquilino.

Observação: se você criar itens de configuração de outro produto da CA Technologies (como o CA APM) ou da interface de linha de comando, o objeto será público.

Mais informações:

Criar um objeto Inquilino. (na página 98)

Criar um objeto Inquilino.

O fornecedor de serviços pode adicionar dados específicos do inquilino a objetos como ocorrências, solicitações, requisições de mudança, e assim por diante. É possível adicionar um inquilino a um ticket (como um incidente) criado a partir da guia Gerenciador de filas.

Par adicionar dados do inquilino a um incidente

1. Clique em Arquivo, Novo incidente.
2. Complete qualquer uma das seguintes etapas:
   a. Selecione o inquilino na lista suspensa Inquilinos.
   b. Clique em Usuário final afetado (ou qualquer outro campo que implique o inquilino).

      A página Pesquisa de contato aparece. Pesquisar um usuário; você pode filtrar a pesquisa por inquilino.
   c. Insira um nome no campo Usuário final afetado.

      Os dados do inquilino são preenchidos automaticamente.
3. Continue a criar o incidente.

Notificações de atividade

Notificações de atividade controlam o conteúdo das notificações e quais contatos receberão notificações para vários eventos no histórico de um ticket.

Em um ambiente de multilocação, a regra de notificação é um objeto opcional para o inquilino. Regras de notificação públicas aplicam-se a todos os tickets, regras alocadas aplicam-se somente a tickets com o mesmo inquilino que a regra ou a inquilinos em sua hierarquia de subinquilinos. A restrição de inquilinos é aplicada em adição a qualquer condição especificada na regra em si.

Mais informações:

Copiar regras de notificação (na página 99)

Copiar regras de notificação

Regras de notificação padrão são armazenadas como objetos públicos. Se a multilocação estiver instalada, é preciso criar uma cópia da Regra de notificação para cada um dos inquilinos, caso contrário a opção Atualizar contatos é restrita.

Para copiar uma regra de notificação

1. Navegue para Notificações, Regras de notificação na guia Administração.

   É exibida a Lista de regras de notificação.

2. Clique em uma regra na coluna Símbolo.

   A página Detalhes da regra de notificação aparece.

3. Clique em Arquivo, Copiar.

   Retome a atualização da regra de notificação.

Repositórios

O objeto repositório (doc_rep) é opcional para o inquilino. Os inquilinos podem definir seus próprios repositórios, e é possível definir repositórios públicos para objetos como anexos para documentos de conhecimento públicos. Cada inquilino pode ter seu próprio repositório padrão e é possível especificar um repositório público padrão.

Todos os anexos são públicos ou associados com um único inquilino. Se um inquilino não tiver seu próprio repositório padrão, o repositório público é exibido como o padrão para seus objetos alocados.

Capítulo 4: Implementando políticas

Esta seção contém os seguintes tópicos:

Implementação de diretivas (na página 101)
Notificações (na página 101)
Administração de email (na página 143)
Contratos de nível de serviço (na página 170)
Segurança (na página 185)
Autenticação de usuário (na página 199)
Logs internos (na página 203)
Integração do CA SDM (na página 203)
Associações de partições de dados (na página 203)
Pesquisas (na página 210)
Web Services (na página 213)

Implementação de diretivas

Um componente chave na configuração de sua central de serviços é a implementação de políticas de modo ideal ao seu atual processo de negócios.

O CA SDM fornece uma implementação de políticas predefinida que é apropriada para alguns locais e serve com um bom ponto de início para outros. Revise a implementação padrão em todas as áreas de definição de políticas para determinar quais partes podem atender às suas necessidades e quais precisam ser modificadas.

Notificações

Com o CA Service Desk Manager, você pode notificar automaticamente pessoas chave sobre atividades de ticket (pesquisa, encaminhamento) e eventos (abertura de um ticket, por exemplo). Também é possível notificar pessoas chave sobre a Ficha de relatório de conhecimento (KRC) e Sessões de assistência do Support Automation. Quando uma atividade ou evento importante ocorre, o CA Service Desk Manager cria uma mensagem de notificação que realiza o seguinte:

- Identifica a atividade de ticket ou o evento de notificação
- Faz referência ao ticket

- Inclui outras informações opcionais
- Pode identificar contatos potenciais

É possível exibir uma mensagem de notificação para um ticket por causa de uma ação de sistema. Uma ação de sistema inclui abrir, fechar ou modificar um ticket por meio de suas informações de histórico.

Definir notificações automáticas envolve as seguintes tarefas:

- Definir notificações de atividade que envolvam os tipos de atividades que geram notificações.
- Definir notificações de contato do objeto que determinam os contatos do objeto que podem ser usados para enviar notificações em uma notificação de atividade.
- Identificar os métodos usados para enviar mensagens.

Mais informações:

Como notificações de atividade funcionam (na página 104)
Notificações de contatos de objeto (na página 105)
Métodos de notificação (na página 106)

Associações de atividades

É possível definir associações de atividades que você pode associar a um atributo de um objeto. As associações de atividade permitem:

- Acompanhar e relatar mudanças no atributo de um objeto.
- Marcar a associação de uma atividade como interna.

  Associações de atividade internas restringem notificações àqueles contatos cujo tipo de acesso permite que exibam logs internos. Os contatos que não sejam autorizados a exibir logs internos não serão notificados, ainda que estejam incluídos como destinatários da notificação. Todos os logs de atividade futuros criados com a atividade associada são marcados como internos.

Observação: um atributo de objeto pode ter somente uma associação de atividade.

Notificações de atividade

Uma atividade é uma ação que alguém realiza, tal como resolver um ticket, enviar uma pesquisa gerenciada, executar a Ficha de relatório de conhecimento, e assim por diante. As notificações de atividade identificam os tipos de atividades que podem acionar uma notificação automática sobre tickets. É possível definir uma notificação para enviar para uma atividade específica. Por exemplo, é possível enviar uma notificação por email para um usuário afetado para obter informações adicionais. O usuário pode responder ao email com as informações solicitadas por um dispositivo como o PDA. Mesmo atividades diárias, como retornar uma chamada, cancelar ou fechar um registro, aumentar uma prioridade ou atualizar o status, podem resultar no envio de uma notificação.

Em geral, notificações de atividades significam o início ou a conclusão de uma ação sobre a qual você quer notificar as pessoas chave, por exemplo, quando tickets são encaminhados, transferidos ou monitorados. Quando uma atividade de ticket ocorre, o CA SDM verifica se a notificação automática está configurada para a atividade. Se ela for selecionada, a notificação de atividade definirá que mensagem enviar ao processo de notificação.

Também é possível executar as ações a seguir em uma notificação de atividade:

- Anexar eventos.
- Criar regras de notificação que definam diretrizes que o sistema deve seguir ao enviar notificações. Por exemplo, definir uma notificação de atividade que notifique o responsável anterior (ou grupo) quando algo for alterado em um ticket.
- Definir uma notificação de atividade manual que atualize um ticket quando o usuário responder.

  Observação: não é possível manter notificações de atividade do tipo Notificação manual diferentes por inquilino, ou copiar uma notificação de atividade do tipo Notificação manual.

Mais informações:

Logs internos (na página 203)
Regras de notificação (na página 114)
Notificações para responsável anterior (na página 133)
Notificações de item de configuração (na página 136)
Como notificações de atividade funcionam (na página 104)

Como notificações de atividade funcionam

Você pode definir uma notificação que é enviada para uma atividade específica. Notificações de atividade podem ser definidas Solicitações, Incidentes, Problemas, Requisições de mudança, Ocorrências, Pesquisas gerenciadas, Documentos de conhecimento, Comentários sobre documentos de conhecimento, Cartão de relatórios de conhecimento, Sessão de assistência, Contatos, Itens de configuração.

Quando você definiu uma notificação de atividade, você pode configurar o seguinte:

Eventos

Define a lista de eventos para essa notificação de atividade. Eventos são procedimentos que um sistema de gerenciamento de ocorrências segue após o transcurso de certo tempo.

Regras de notificação

Define novas regras de notificação para solicitações/incidentes/problemas, requisições de mudança, ocorrências. Você também pode modificar as regras padrão que aparecem na lista Regras de notificação.

Pesquisa

Define uma notificação de pesquisa que permitirá ao destinatário desta notificação de atividade clicar em um URL para exibir uma pesquisa. As pesquisas permitem coletar e analisar comentários do cliente.

Observação: para obter mais informações sobre a criação de notificações de atividade para Solicitações, Requisições de mudança, Ocorrências, Pesquisas gerenciadas, Documentos de conhecimento, Comentários de documentos de conhecimento, Cartão de relatório de conhecimento, Sessão de assistência, Contatos ou Itens de configuração, consulte a *Ajuda online*.

Notificações de contatos de objeto

As notificações de contatos do objeto permitem notificar destinatários com base no valor atual de um campo no ticket. Em vez de identificar uma pessoa para notificar, como em um método de notificação, você identifica um objeto. Por exemplo, você pode identificar o campo Para para assegurar que essa notificação vai para a pessoa atualmente identificada no campo Para, ainda que o valor tenha sido alterado desde que o ticket foi definido.

Para criar uma notificação de contato de objeto

1. Na guia Administração, selecione Notificações, Notificações de contato do objeto.

   A página Lista de notificação de contato do objeto é exibida.

2. Clique em Criar novo.

   A janela Criar nova notificação de contatos de objeto é exibida.

3. Preencha os seguintes campos:

   Símbolo

   Define um identificador exclusivo para a notificação de contato de objeto.

   Status

   Especifica se a notificação de contato de objeto está ativa ou inativa.

   Tipo do objeto

   Exibe o nome do objeto ao qual o atributo se aplica.

   Nome do atributo de objeto

   Fornece o nome da notificação de contato de objeto (no campo Símbolo) em Majic, que é o código interno da CA. O nome do atributo depende da seleção Tipo de objeto:

   - Se o tipo de objeto for Ocorrência ou Tarefa do fluxo de trabalho, o nome do atributo será destinatário, solicitante ou grupo; esses são os nomes do atributo nos objetos de mudança e eles mapeiam campos nas tabelas Change_Request.

- Se o tipo de objeto for um log de atividades da ocorrência, o nome do atributo deverá se iniciar com o nome do atributo no objeto log de atividades que o vincula a uma instanciação específica do objeto chg. O nome de atributo pode ser change_id.group.

Descrição

Descreve a notificação de contato de objeto.

4. Clique em Salvar.

   A nova notificação de contato do objeto é exibida na Lista de notificações de contatos de objeto ao exibir novamente a lista.

Observação: para obter mais informações sobre como configurar as notificações do contato do objeto, consulte a *Ajuda online*.

Métodos de notificação

Os métodos de notificação descrevem como as mensagens de notificação são enviadas aos usuários. Os métodos de notificação são scripts ativados de acordo com as notificações de atividade. Os scripts usam informações fornecidas como variáveis para notificar a equipe ou outros sistemas sobre a ocorrência de m evento. Por exemplo, você pode criar um script que envie mensagens de voz ao analista atribuído a uma solicitação para indicar que a solicitação foi encaminhada a um nível superior.

Métodos de notificação podem ser atribuídos a cada registro de contato. O sistema procura o método de notificação a usar com contatos específicos.

Os métodos de notificação padrão do CA SDM são os seguintes:

- Email:mensagens são enviadas por email diretamente ao destinatário usando SMTP (Simple Mail Transport Protocol). As mensagens também são enviadas ao log de notificação do destinatário.
- A função de notificação envia mensagens ao log de notificação do destinatário, que pode ser acessado durante a execução do CA SDM.
- O email do pager envia email a um endereço mantido por um provedor de sistema de pager. Em geral, o texto de email pode ser exibido em um pager alfanumérico.

Você também pode criar seus próprios métodos de notificação. Por exemplo, você pode enviar uma notificação a uma impressora particular para a coleta periódica ou a um pager. Para criar um método de notificação, crie um script de shell que inclua variáveis de notificação e, em seguida, armazene o novo método de notificação no CA SDM.

Observação: para obter mais informações sobre métodos de notificação, consulte o *Guia de Implementação*.

Mais informações:

Configuração de notificação com base no tipo de contato (na página 218)

Utilitário pdm_mail - Enviar notificação de email

O utilitário pdm_mail é usado em notificações para enviar emails, ao enviar informações de email para o processo pdm_mail_nxd. O utilitário pdm_mail também pode ser usado para comandos, mas não para ambos. Se nenhum parâmetro for usado, então o comportamento padrão de usar a variável NX_NTF_xxxx para passar parâmetros está em vigor.

Para email, o utilitário é invocado da seguinte maneira:

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H] [-N]
[-R] [-h]
```

-i

Usa STDIN em vez de variáveis NTF. Os seguintes parâmetros são usados apenas para comportamento de email STDIN:

-e

Especifica o endereço de email (para o destinatário).

-s

Especifica o assunto do email.

-q

Desabilita o prompt de exibição para STDIN.

-p

Usa lógica de pager. Esta opção inclui o uso do endereço de email do pager em vez do endereço de email normal. Somente a versão de texto sem formatação da notificação é usada (sem HTML).

-M

Usa somente texto sem formatação (sem MIME) no corpo

[-f]

Especifica o endereço De do email.

-T

Especifica o endereço Reply-To do email.

-B

Especifica o conjunto de caracteres do corpo. Pode ser útil para pagers que não oferecem suporte a UTF-8.

-H

Especifica o conjunto de caracteres do cabeçalho. Pode ser útil para pagers que não oferecem suporte a UTF-8.

-N

Especifica a opção de notificação DSN (Delivery Status Notification - Notificação de Status de Entrega).

-R

Especifica a opção de retorno DSN.

-h

Exibe ajuda no utilitário.

Para comandos, o utilitário é invocado da seguinte forma:

Comando para o servidor de correio

```
pdm_mail -c option [parameter]
```

Comando para o mail eater

```
pdm_mail -x option [parameter]
```

check_interval

(somente -x) Modifica o intervalo de verificação de correio para um valor especificado (em segundos).

report_interval

Modifica o intervalo de relatório para um valor especificado (em segundos).

report_now

Determina o envio de um relatório para os logs. O contador não é redefinido.

send_q

(somente -c) Envia a fila de correio local para o servidor de correio remoto.

trace

Liga ou desliga o rastreamento.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira "pdm_task pdm_clean_attachments...".

Notificações de email

Notificações de email ajudam os analistas a comunicar-se com funcionários e usuários finais.

Funcionários e usuários finais em um ambiente algumas vezes são remotos, e interagem com o CA SDM usando email. É possível configurar o CA SDM de modo que esse tipo de usuário possa fazer o seguinte:

- Atualizar uma solicitação/incidente/problema/requisição de mudança/ocorrência através de uma resposta a uma notificação de email enviada do CA SDM.
- Aprovar ou rejeitar uma tarefa do workflow (clássica ou do CA Workflow) usando email.

Notificações permitem que você se comunique com os interessados para um ticket da seguinte maneira:

- Notificações de email podem mostrar todos os destinatários da notificação, informando o usuário sobre quais são as partes interessadas.
- Os analistas podem enviar uma notificação manual para um endereço de email temporário que atualmente não está associado a um contato. Um endereço temporário é útil, por exemplo, quando um usuário final está fora do escritório ou está com dificuldade para acessar sua conta de email padrão.
- Os analistas podem enviar anexos com uma notificação para comunicar detalhes adicionais a um usuário.

Endereços de email temporários

Um endereço de email temporário é aquele que não está associado a um contato no sistema.

Endereços de email temporários são úteis em circunstâncias como a seguinte:

1. Um usuário final está fora do escritório ou está com dificuldades em acessar sua conta padrão de email.
2. O analista deseja usar o email para acompanhar interações com o usuário.
3. O analista envia uma notificação manual para o endereço de email *temporário* para o usuário.
4. O analista pode visualizar o log de atividade, que é atualizado com a notificação manual.

Observação: para obter mais informações sobre como configurar endereços de email temporários, consulte a *Ajuda online*.

Permitir endereços de email temporários

Você pode permitir que os usuários enviem notificações manuais a endereços de email temporários. Por exemplo, os analistas podem enviar email a endereços que não estão associados a um registro de contato. Os destinatários não podem responder a endereços de email temporários quando seus endereços de email não estão associados a um registro de contato ou não possuem permissão para atualizar o ticket.

Observação: endereços de email temporários são sempre endereços de email SMTP e têm suporte somente quando o Método preferencial oferece suporte a SMTP.

Para permitir endereços de email temporários

1. Na guia Administração, navegue até o Gerenciador de opções, Notificações.

   A Lista de opções aparece.

2. Clique em notification_allow_temp_address.

   A página Detalhes de opções notification_allow_temp_address aparece com os valores padrão definidos.

3. Clique em Editar.

   A página Atualizar opções notification_allow_temp_address aparece com os valores padrão definidos e você pode editar a Descrição.

4. Clique em Instalar.

   A página Detalhes de opções notification_allow_temp_address aparece.

5. Clique em Fechar janela.

6. Reinicialize o servidor do CA SDM.

   Endereços de email temporários não têm permissão para notificações manuais.

Proibir endereços de email temporários

Por padrão, os usuários não podem enviar manualmente notificações de atividade a endereços de email temporários. Por exemplo, os analistas não podem enviar email a endereços que não estão associados a um registro de contato. Os administradores instalam a opção notification_allow_temp_address para permitir endereços de email temporários. Se a opção estiver instalada e você desejar cancelar a permissão para notificações manuais para endereços de email temporários, é possível desinstalar a opção.

Observação: endereços de email temporários usam endereços de email SMTP e o método de notificação Método preferencial.

Para cancelar temporariamente a permissão endereços de email

1. Na guia Administração, navegue até o Gerenciador de opções, Notificações.

   A Lista de opções aparece.

2. Clique em notification_allow_temp_address.

   A página Detalhes de opções notification_allow_temp_address aparece.

3. Clique em Editar.

   A página Atualizações opções de notification_allow_temp_address é exibida.

4. Clique em Desinstalar.

   A página Detalhes de opções notification_allow_temp_address aparece.

5. Clique em Fechar janela.

6. Reinicialize o servidor do CA SDM.

   A opção é desinstalada e endereços de email temporários agora têm permissão cancelada para notificações manuais de atividade;

Polling de caixa de correio

Se ocorrer um erro no servidor de correio de envio, as notificações de email não são enviadas e colocadas na fila no diretório %NX_ROOT%\site\mail_queue. Quando o servidor de correio fica ativo novamente, após um intervalo, ele processa e envia o email. Você pode alterar o intervalo para reciclar o email que foi colocado na fila quando o servidor de correio estava ocupado.

Mensagens de email de notificação que o servidor de correio de envio falha em enviar são reenviadas até que você faça um dos seguintes:

- Para o Mail Daemon (pdm_mail_nxd) que opera notificações de email enviado.
- Exclui manualmente as mensagens do diretório %NX_ROOT%\site\mail_queue.

Definir a variável de intervalo de novas tentativas de email

É possível definir o intervalo de tempo (em segundos) para fazer novas tentativas que falharam para enviar email de saída para o servidor de correio.

Observação: o CA SDM não tenta reenviar mensagens que o servidor de correio de saída aceita, mas não podem ser entregues. Para essas mensagens, os recursos e políticas de nova tentativa do servidor de email de envio, se houver, estão em vigor.

As novas tentativas são feitas por mensagem. Se o servidor de correio estiver indisponível por um tempo, cada mensagem é repetida quando seu próprio temporizador expira, em vez de todas as mensagens serem enviadas de uma vez. Entretanto, se você reiniciar o daemon de correio de saída, todas as mensagens não enviadas tentam ser enviadas naquele momento, e se todas falharem em ser enviadas, seus timers de novas tentativas são todos redefinidos ao mesmo tempo.

A configuração (NX_EMAIL_RETRY_INTERVAL) no arquivo NX.env controla o intervalo de novas tentativas. É possível alterar a configuração do intervalo de novas tentativas padrão em um ou mais servidores.

Para definir o intervalo de novas tentativas de email

1. Navegue para o diretório $NX_ROOT no servidor.
2. Use um editor de texto como o WordPad para abrir o arquivo NX.env.
3. Modifique o valor para o intervalo NX_EMAIL_RETRY_INTERVAL que você deseja como segue:

   ```
   NX_EMAIL_RETRY_INTERVAL=number_of_seconds
   ```

   NX_EMAIL_RETRY_INTERVAL

   Define o intervalo de tempo (em segundos) para repetir tentativas de email que falharam.

   number_of_seconds

   Especifica o número de segundos para cada intervalo de novas tentativas de email. O valor padrão são 600 segundos (10 minutos). O valor mínimo que você pode usar são 20 segundos. Se você definir um valor inferior ao valor mínimo de 20 segundos ou acima de 2.000.000 de segundos, será usado o valor padrão de 10 minutos.

4. Salve e feche o arquivo.
5. Reinicie o serviço do CA SDM.

   A mudança entra em vigor.

Regras de notificação

Uma regra de notificação define diretrizes para o sistema seguir ao enviar notificações. Usando regras de notificação, você pode especificar quem deve ser notificado automaticamente e em que circunstâncias.

É possível definir regras de notificação para solicitações, incidentes, problemas, requisições de mudança, ocorrências, contatos, itens de configuração e inquilinos globais e específicos. Cada regra de notificação contém os seguintes componentes:

Macro de condição

Configure para representar os valores desejados de um ou mais campos de um ticket de central de serviço. A condição é avaliada em diferentes pontos durante o processamento para determinar se uma ação ocorre.

Modelo de mensagem

Contém um protótipo da mensagem que é gerada e enviada a contatos quando a notificação é enviada. Uma regra de notificação deve conter um modelo de mensagem, e eles podem ser reutilizados.

Contatos de objeto

Exibe o contato do objeto derivado das informações do ticket, como o responsável, usuário final, grupo e assim por diante. Se a condição é satisfeita, esses contatos do objeto recebem a notificação.

Contatos

Se a condição é satisfeita, esses contatos recebem a notificação. Os contatos são os registros do banco de dados que representam os usuários do sistema.

Tipos de contato

Exibe o tipo dos contatos que você deseja que recebam a notificação por padrão, por exemplo, Analistas, Funcionário, Cliente e assim por diante.

Notificações de atividade relacionadas

Exibe uma lista de notificações de atividade relacionadas que usam a regra de notificação.

Observação: os usuários podem receber várias notificações para uma notificação de atividade que contenha várias regras para as quais eles atendem às condições.

Opções de configuração de regras de notificação

É possível especificar as seguintes opções ao definir uma regra de notificação:

- **Regra de notificação padrão**—É possível especificar uma regra padrão de notificação que automaticamente notifica todos os contatos identificados no campo referenciado no ticket. Para exibir a lista de regras padrão de notificação que podem ser modificadas, selecione a guia Administração, Notificações, Regras de notificação.
- **Macro de condição definida pelo local**—É possível implementar uma *macro de condição definida pelo local* para criar sua própria condição que notifica somente contatos sob certas circunstâncias. Para criar uma macro de condição a partir da guia Administração, selecione Eventos e Macros, Tipos de Macro e, a seguir, Condição definida pelo site na lista de Tipo de macro.
- **Novos contatos**—Ao definir uma regra de notificação, é possível identificar novos contatos para receber notificações nas seguintes guias:
  - **Contatos de objeto—**Exibe organizações, fornecedores e itens de configuração disponíveis para o tipo de objeto selecionado que receberá a notificação sobre tickets.
  - **Contatos—**Exibe os indivíduos adicionados à regra de notificação, independentemente de sua relação com o ticket.
  - **Tipos de contato—**Exibe os usuários definidos na regra de notificação com a mesma classificação, como analista ou cliente.

  O botão Atualizar em cada guia permite pesquisar por novos registros de contato associados com a regra.

  Observação: antes de implementar uma regra de notificação, configure os contatos apropriados para sua estrutura comercial.
- **Modelo de mensagem**—Toda regra de notificação deve conter um modelo de mensagem. É possível definir seu próprio modelo de mensagem ou especificar um dos modelos padrão de mensagem disponíveis na página da lista de Modelos de mensagem. Para exibir esta página, selecione a guia Administração, Notificações, Modelos de mensagem.
- **Notificações de item de configuração**—Quando você define uma regra de notificação, é possível identificar a pessoa responsável por manter um item de configuração para receber notificações quando um ticket é criado.
- **Notificações para o destinatário anterior**—Ao definir uma notificação de atividade, é possível especificar valores na regra de notificação que notifiquem o destinatário ou grupo anterior quando uma atividade de evento ocorre.

Mais informações:

Como definir a estrutura comercial (na página 65)
Exemplo: criar um modelo de mensagem (na página 125)
Notificações para responsável anterior (na página 133)
Notificações de contatos de objeto (na página 105)
Visão geral da macro de condição definida pelo local (na página 116)

Visão geral da macro de condição definida pelo local

Um gerente deseja ser informado sobre todas as atividades de tickets que ocorrem para ocorrências de Prioridade 2 relacionadas a seu departamento. O administrador adiciona o gerente como contato específico nos tipos selecionados de notificações de atividade, como Inicial e Comentário de log. Com esta implementação, o gerente recebe todas as notificações de atividade selecionadas para todo o sistema.

Em um departamento com alto volume, como o suporte técnico, o tráfego indesejado de email pode ser significativo. Para controlar suas caixas de correio, o gerente deve implementar regras de caixa de correio para filtrar as notificações e esperar que nada importante seja perdido.

O administrador define uma macro de condição definida pelo local que somente notifica o gerente quando a Prioridade é definida como 2 e a Área de solicitação é definida como Aplicativos (departamento do gerente). A nova condição é especificada na regra de notificação e o gerente é adicionado como o contato. É definido um modelo de mensagem que descreve a atividade do ticket e a regra é adicionada à notificação da atividade.

A atividade ocorre quando a prioridade de um ticket é definida como 2 e a área de solicitação é definida como Aplicativos. Quando esta atividade ocorre, a regra é implementada e a condição é avaliada. Se a condição avaliar como Verdadeira, uma mensagem de notificação descrevendo a atividade do ticket é enviada para o gerente. Notificações indesejadas não são mais enviadas para o gerente.

Exemplo de regra de notificação

Os exemplos de regra de notificação fornecem informações introdutórias para ajudá-lo a fazer o seguinte:

- Criar uma macro de condição definida pelo local
- Criar uma regra de notificação
- Adicionar a regra à notificação de atividade

Quando a atividade ocorre, a respectiva condição vinculada à regra é implementada. Se a condição for atendida (avaliar como *verdadeira*), uma mensagem de notificação que descreve a atividade do ticket é enviada a todos os contatos.

Mais informações:

Exemplo: criar uma macro Condições definidas pela localidade (na página 117)
Exemplo: criar uma regra de notificação (na página 119)
Exemplo: adicionar a regra para a notificação de atividade (na página 120)

Exemplo: criar uma macro Condições definidas pela localidade

Neste exemplo, você cria uma macro de condição definida pela localidade que verificará a condição especificada.

1. Na guia Administração, vá para Eventos e macros, Macros.

   A página Lista de macros aparece.

2. Clique em Criar novo.

   A página Criar nova macro aparece.

3. Preencha os seguintes campos:

   - Símbolo: insira *Application P1*.
   - Tipo de macro: selecione Condições definidas pela localidade.
   - Tipo de objeto: selecione solicitação.

4. Clique em Continuar.

   A página Create New Macro Applications P1é exibida.

5. Preencha os seguintes campos:
   - Descrição da macro: digite *Macro=Solicitação, Prioridade=1, Área de solicitação=Aplicativos*.
   - Se todas as Condições retornarem com sucesso: selecione TRUE.
   - Status do registro: selecione Ativo
6. Clique em Salvar.

   A página Applications 1 Macro Detail é exibida.
7. Clique em Adicionar condição.

   A página Criar nova condição Atomic aparece.
8. Crie uma condição Atomic para verificar a Prioridade=2 e preencha os seguintes campos:
   - Sequência: digite *10*.
   - Descrição: digite *Verificar a prioridade*.
   - Selecione um atributo: selecione Prioridade.
   - Escolha o operador: selecione igual a.
   - Selecione o atributo ou valor de dados: selecione valor de dados.
9. Selecione 2 para o valor de dados e clique em Salvar.
10. A partir da página Detalhes da macro, clique em Adicionar condição e preencha os seguintes campos:
    - Sequência: digite *20*.
    - Descrição: digite *Verificar área de solicitação=Aplicativos.*
    - Selecione um atributo: Selecionar área de solicitação.
    - Escolha o operador: Selecione igual a.
    - Selecione o atributo ou valor de dados: Selecione valor de dados.
11. Selecione Aplicativos para o valor de dados e clique em Salvar.

    A nova condição é exibida na guia Condições da macro de condições definidas pela localidade.

Exemplo: criar uma regra de notificação

Neste exemplo, você associará a macro de condição definida pela localidade à regra de notificação, anexará um modelo de mensagem e adicionará Gerente como um tipo de contato.

1. Na guia Administração, vá para Notificações, Regras de notificação.

   A página Lista de regras de notificação aparece.

2. Clique em Criar novo.

   A página Criar regras de notificação aparece.

3. Preencha os seguintes campos:

   - Símbolo: digite Notificar gerentes sobre App1.
   - Tipo de objeto: selecione solicitação.
   - Descrição: digite *notificar gerentes sobre interrupção de aplicativo de prioridade 1*.

4. Clique em Salvar e continuar.

5. Clique no link Condição e selecione a nova macro de condições definidas pela localidade chamada Application P1.

6. Clique em Modelo de mensagem.

   A página Lista de modelos de mensagem aparece.

7. Selecione uma mensagem a partir da lista Certifique-se de que a opção Notificação automática está ativada no modelo de mensagem.

8. Na guia Tipos de contato, clique no botão Atualizar tipo de contato.

   A página Pesquisa de tipo de contato aparece.

9. Clique em Pesquisar.

   A lista Destinatários da regra de notificação é exibida.

10. Selecione Gerenciador na lista à esquerda e clique no botão de seleção de contatos (> >).

11. Quando o contato estiver na lista da direita, clique em OK.

12. Salve a regra de notificação.

    A nova regra de notificação aparece na Lista de regras de notificação quando você exibe novamente a lista.

Exemplo: adicionar a regra para a notificação de atividade

Neste exemplo, você ativará a opção Notificação automática no modelo de mensagem e adicionará a regra de notificação à notificação de atividade.

1. Na guia Administração, vá para Notificações, Notificações de atividade.

   A página Lista de notificações de atividade aparece.

2. Selecione a notificação de atividade inicial na lista.

   A página Initial Activity Notification Detail aparece.

3. Verifique se o Tipo de objeto está definido para Solicitações, de modo que o bloco de notas apareça nas informações de configuração para solicitações.

4. Na guia Regras de notificação, clique em Atualizar regras de notificação.

   A página Pesquisa de regras de notificação aparece.

5. Digite *Gerenciador de notificação de App P1* no campo Símbolo e clique em Pesquisar.

   A página Notification Rules Assigned Update aparece.

6. Selecione *Gerenciador de notificação de App P1* na lista da esquerda e clique no botão de seleção de contatos (>>).

   A regra de notificação está na lista à direita.

7. Clique em OK.

8. Clique no link Condição e selecione a nova regra de notificação Gerenciador de notificação de App P1. (Você pode adicionar regras adicionais clicando no botão Atualizar regras de notificação.)

   A página Notificação de atividade aparece.

9. Certifique-se de que a opção Notificação automática está ativada no modelo de mensagem como segue:

   a. Clique no link Regra de notificação na guia da notificação de atividade.

      A página Regras de notificação é exibida.

   b. Clique no log Modelo de mensagem.

      A página Detalhes do modelo de atualização aparece.

c. Clique em Editar.

   A página Atualizar modelo de mensagem aparece.

d. Verifique se Notificação automática está ativada.

10. Clique em Salvar.

    Quando a atividade ocorre, a respectiva condição vinculada à regra é implementada. Se a condição for alcançada (avalia como verdadeiro), uma mensagem de notificação que descreve a atividade do ticket é enviada a todos os gerentes.

Exemplo de regras de notificação padrão

O CA SDM contém várias regras de notificação padrão. É possível exibir as regas de notificação padrão navegando para Notificações, Regras de notificação na guia Administração.

Mais informações:

Exemplo: usar a regra de solicitação com prioridade 1 (na página 121)
Exemplo: usar a regra Notificar o responsável atual e anterior de uma requisição de mudança. (na página 123)
Exemplo: usar a regra Escalonamento com prioridade verdadeira (na página 123)
Exemplo: usar a regra de solicitação/incidente/problema ativa. (na página 124)

Exemplo: usar a regra de solicitação com prioridade 1

As regras de notificação fornecem flexibilidade ao usuário final se desejarem receber uma notificação em relação a uma solicitação com prioridade 1. A regra de *Solicitação com prioridade 1* é executada se o tipo de ticket for uma solicitação e a prioridade estiver definida como 1. Essa notificação é enviada somente quando a condição vinculada à regra é avaliada como verdadeira e usa o modelo de mensagem vinculado à regra.

Observação: é possível modificar o modelo de mensagem de uma Regra de notificação abrindo a regra a modificando o campo Condição com uma macro. Para obter mais informações sobre a modificação de condições, consulte a *Ajuda online*.

O produto também contém Regras de notificação padrão chamadas Incidente com prioridade 1 e Problema com prioridade 1. As principais diferenças entre essas regras e a Solicitação com prioridade 1 são as condições para os tipos de tickets. Por exemplo, Solicitação com prioridade 1 tem a condição com uma sequência "20" vinculada a ela que limita a regra de notificação somente a solicitações.

Por padrão, nenhum contato, contato de objeto ou tipo de contato é vinculado à regra. O campo "Notificação automática" no modelo de mensagem vinculado à regra também é definido como Não por padrão. Para enviar uma notificação, é necessário adicionar um Contato de objeto ou Contato, ou Tipo de Contato à regra e o campo Notificação automática no Modelo de mensagem deve ser alterado para Sim.

Exemplo: configurar uma regra para enviar uma notificação somente para Solicitações com prioridade definida para 1

A regra deveria estar conectada tanto à Notificação de atividade Inicial quanto de Escalonar. Isso ajuda a garantir que as notificações sejam recebidas para uma nova Solicitação com prioridade 1 e que a Solicitação seja escalonada para uma prioridade 1.

1. Verifique se a regra padrão vinculada à notificação de atividade Inicial e Escalonar foi removida ou se a opção Notificação automática está definida como Não.

   Isso evita que a notificação seja enviada para essas regras padrão.

2. Abrir a regra Solicitação com prioridade 1.
3. Adicione um Contato de objeto ou um contato ou um Tipo de contato à regra.
4. Clique no Modelo de mensagem e selecione a opção Notificação automática.
5. Vincule a regra Solicitação com prioridade 1 às notificações de atividade Inicial e Escalonar.
6. Faça o seguinte:
   - Crie uma nova solicitação e defina a prioridade para 1.

     Verifique se o usuário recebeu a notificação.
   - Crie uma nova solicitação e defina a prioridade para uma prioridade diferente, como 2.

     Verifique se o usuário não recebe a notificação.

Exemplo: usar a regra Notificar o responsável atual e anterior de uma requisição de mudança.

A regra *Notificar o responsável atual e anterior de uma requisição de mudança* notifica tanto o responsável atual quanto o anterior sobre a requisição de mudança durante uma transferência. Também é possível criar uma regra similar para outros tipos de ticket.

Exemplo: notificar os responsáveis atual e anterior de uma transferência de requisição de mudança

1. Verifique se a regra padrão vinculada à notificação de atividade inicial foi removida ou se "Notificação automática" no modelo de mensagem vinculado à regra está definida como Não.

   Isto impede que as notificações sejam enviadas de acordo com estas regras padrão.

2. Abra a regra Notificar o responsável atual e anterior de uma requisição de mudança.

3. Clique no modelo de mensagem Notificar o responsável atual e anterior de uma requisição de mudança e selecione a opção Notificação automática.

4. Vincule a regra Notificar o responsável atual e anterior de uma requisição de mudança à notificação de atividade de Transferência.

5. Faça o seguinte:

   a. Crie e salve uma requisição de mudança com um responsável.

   b. Transfira para o novo responsável.

   Verifique se ambos os usuários receberam a notificação de transferência.

Exemplo: usar a regra Escalonamento com prioridade verdadeira

A Notificação de atividade Escalonar ocorre quando a prioridade de um ticket é alterada, não apenas quando a prioridade aumenta. Os usuários são notificados de escalonamentos, bem como de desescalonamentos. As Regras de notificação agora fornecem uma maneira de discriminar entre uma mudança de prioridade 2 para prioridade 1 e uma mudança de prioridade 1 para prioridade 2

A regra *Escalonamento com prioridade verdadeira* avalia os valores atual e anterior do campo Prioridade. Esta regra notifica o contato de objeto, o contato e os tipos de contato vinculados à regra somente quando a prioridade de um ticket de ocorrência for alterada de uma prioridade mais baixa para uma prioridade mais alta.

Observação: você pode criar uma regra similar para outros tipos de ticket. A notificação é enviada somente quando a condição vinculada à regra for avaliada como verdadeira e usar o modelo de mensagem vinculado à regra. Por padrão, nenhum contato, contato de objeto ou tipo de contato é vinculado à regra. O campo Notificação automática no modelo de mensagem vinculado à regra também é definido como Não por padrão.

Exemplo: receber informações quando a prioridade é alterada de uma prioridade menor para uma prioridade maior para um tipo de ticket de Ocorrência

1. Verifique se a regra padrão vinculada à notificação de atividade Escalonar foi removida ou se a opção Notificação automática no modelo de mensagem vinculado ao padrão está definida como Não.

   Isso evita que sejam enviadas notificações para essas regras padrão.

2. Abra a regra Escalonamento com prioridade verdadeira.

   Adicione um Contato de objeto ou um contato ou um Tipo de contato à regra.

   Verificar se o Contato pode receber notificações.

3. Clique no campo Escalonamento com prioridade verdadeira no Modelo de mensagem e verifique a opção Notificação automática.

   Vincular a regra à notificação de atividade de Escalonamento.

4. Criar uma nova ocorrência com uma prioridade, como 5.
5. Alterar a prioridade para 4 e verificar se o usuário recebeu a notificação.
6. Alterar a prioridade de 4 para 5 e verificar se o usuário não recebeu a notificação.

Exemplo: usar a regra de solicitação/incidente/problema ativa.

A regra *Solicitação/incidente/problema ativo* tem uma condição vinculada para avaliar o envio da notificação inicial somente se a solicitação/incidente/problema estiver ativo.

Isso permite ao cliente receber somente a notificação de Fechamento quando uma solicitação inativa é criada. Esta regra notifica o contato de objeto/contato e tipos de contato vinculados à regra somente quando uma solicitação/incidente/problema ativa for criada.

Observação: é possível criar uma regra similar para requisições de mudança e ocorrências de tipos de ticket.

A notificação é enviada somente quando a condição vinculada à regra é avaliada como verdadeira e usa o modelo de mensagem vinculado à regra. Por padrão, nenhum contato, contato de objeto ou tipo de contato é vinculado à regra. Além disso, o campo "Notificação automática" no modelo de mensagem vinculado à regra também é definido como Não por padrão.

Exemplo: receber uma notificação quando você fecha um Incidente

1. Verifique se a regra padrão vinculada à notificação de atividade inicial foi removida ou se "Notificação automática" no modelo de mensagem vinculado à regra padrão que, por sua vez, está vinculada a notificações de atividade Escalonar, está definida como Não.

   Isto impede que as notificações sejam enviadas de acordo com estas regras padrão.

2. Abra a regra de solicitação/incidente/problema ativa.

   Adicione um Contato de objeto ou um contato ou um Tipo de contato à regra.

   Verifique se o Contato pode receber notificação.

3. Clique no modelo de mensagem Solicitação/incidente/problema ativo vinculado à regra e marque a caixa de seleção Notificação automática.
4. Vincular a regra de solicitação/incidente/problema ativa à notificação de atividade Inicial.
5. Criar um novo Incidente e definir o campo status para Fechado.
6. Verificar se o usuário designado configurado para receber a notificação não recebeu a notificação Inicial.

Exemplo: criar um modelo de mensagem

Toda regra de notificação deve conter um modelo de mensagem. Você pode criar modelos que contenham valores padrão para usar em mensagens de notificação.

Exemplo: criar um modelo de mensagem

Este exemplo demonstra como criar um modelo de mensagem.

Para criar um modelo de mensagem

1. Na guia Administração, vá para Notificações, Modelos de mensagem.

   A Lista de modelos de mensagem aparece.

2. Clique em Criar novo.

   A janela Criar modelo de mensagem aparece.

3. Preencha os seguintes campos:

   Inquilino

   Especifica o inquilino associado a esse modelo.

   Observação: selecionar global (compartilhado) permite usar o modelo para mensagens globais.

   Símbolo

   Define um identificador exclusivo para esse registro.

   Tipo do objeto

   Especifica o tipo de objeto associado a esse modelo.

   Status do registro

   Especifica ou inativo para o status desse modelo.

   Notificação automática

   Especifica se a notificação associada ao modelo será enviada automaticamente quando a atividade ocorrer.

   Nível de notificação

   Indica a importância relativa do envio dessa notificação. Selecione: Emergência, Alto, Baixo ou Normal.

   Título da mensagem de notificação

   Especifica o título resumido da mensagem. Você pode usar variáveis para inserir valores do ticket quando uma notificação é enviada. Por exemplo, você pode incluir uma variável que insira o número da ocorrência no título da mensagem.

   Corpo da mensagem de notificação

   Especifica o conteúdo da mensagem. Você pode usar variáveis para inserir valores do ticket quando uma notificação é enviada. Por exemplo, você pode usar uma variável que insira o nome do analista, o nome do usuário final e uma descrição na mensagem.

Mensagem HTML

Especifica uma mensagem em HTML para ser exibida se o programa de email do destinatário suportar mensagens HTML. Se o destinatário receber a mensagem em um dispositivo portátil, como um telefone celular ou Blackberry, a mensagem será exibida somente em texto sem formatação.

Editar mensagem HTML

Abre o Editor de HTML, que permite editar sua mensagem HTML.

Exibição rápida

Exibe a mensagem como ela aparecerá para o destinatário.

Código-fonte HTML

Exibe a mensagem em código-fonte HTML.

4. Clique em Salvar.

   O novo modelo de mensagem aparece na Lista de modelos de mensagem.

Objetos em mensagens

Você pode usar a palavra-chave ARTIFACT para especificar como os objetos são processados em mensagens enviadas, modelos de mensagem, notificações e respostas automáticas. A palavra-chave ARTIFACT usa os seguintes valores:

- **NONE-**Especifica nenhuma validação de artefatos Esse valor é o mesmo que não usar a palavra-chave.
- **PROTECTED**—Valida um ticket contra o hash de confirmação. Se a confirmação falha, o objeto é considerado inválido e a filtragem falha quando pesquisa um objeto ({{object_id}}).
- **SECURE** — descriptografa o número do ticket. Se o valor não é uma senha válida, o objeto é considerado inválido e a filtragem falha quando está procurando um objeto ({{object_id}}).

Códigos e frases de notificações

Frases de notificação permitem adicionar uma parte de uma informação padronizada ou texto a diversas mensagens de notificação diferentes sem necessidade de inserir e manter o texto ou fórmula separadamente em cada modelo de notificação. Por exemplo:

Responda a esta notificação para acrescentar informações adicionais ao ticket

Frases padronizam texto para uso em diversos modelos de mensagem. Por exemplo, é possível manter uma frase comum, como um aviso confidencial em um único registro e usá-la em diversos modelos de mensagem. Frases de notificação também são úteis para respostas a mensagens, como Reply Notice, ou um link de URL da web. O CA SDM fornece frases e você pode criar suas próprias frases. É possível definir uma frase como ativa ou inativa para uso em um modelo de mensagem globalmente. (Frases de notificação estão inativas por padrão.) Quando uma frase está inativa, ela é suprimida em todos os modelos de mensagem que usam a frase.

Frases de notificação também podem ser usadas nas respostas automáticas para mensagens de email recebidas. O contexto de processamento para esse tipo de mensagem é diferente; omite o prefixo (change_id., issue_id., call_req_id.) usado em determinadas macros, como ref_num e web_url para frases que a mensagem usa. Como resultado, não é possível compartilhar frases de notificação entre modelos de notificação e respostas automáticas de email.

Por exemplo, algumas das frases que o CA SDM fornece são da seguinte maneira:

Símbolo	Código	Frase
Histórico de notificação - Mudança	notify_history_chg	Clique no URL a seguir para exibir a Lista de notificação: @{change_id.web_url}+HTMPL=chg_lr.htmpl +INSTANCE=@{id}
Histórico de notificação - Ocorrência	notify_history_iss	Clique no URL a seguir para exibir a Lista de notificação: @{issue_id.web_url}+HTMPL=iss_lr.htmpl+INSTANCE=@{id}

Símbolo	Código	Frase
Histórico de notificação - Solicitação/incidente/problema	notify_history_cr	Clique no URL a seguir para exibir a Lista de notificação: @{call_req_id.web_url}+HTMPL=cr_lr.htmpl+INSTANCE=@{id}

Exemplo: novas frases

As frases a seguir são exemplos de frases podem ser criadas:

Símbolo	Código	Frase
Notificação de confidencialidade	ConfidentialNotice	This email and any files transmitted with it are for the sole use of the intended recipient(s) and contain information that may be privileged and confidential. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient of this email, please delete this email and any files transmitted with it and notify the sender immediately.
Resposta para notificação de incidente	IncidentReply	To add a comment to your Incident, just reply to this email or include the line below (on a line by itself). %incident_id=@{call_req_id.ref_num}
URL de notificação de incidente	IncidentURL	Click the following URL to view: @{call_req_id.web_url}

Observação: use frases separadas para versões de texto sem formatação e HTML de modelos de mensagem ou respostas automáticas de email. HTML consolida a maioria dos espaços em branco em espaços únicos, então quebras de linhas, ou de parágrafo, devem ser especificadas com marcas. Marcas HTML inclusas em versões de texto sem formatação de mensagens são exibidas, em vez de processadas.

Sintaxe de frase de notificação

Você insere frases de notificação nos modelos de mensagem e envia por email mensagens de resposta usando a seguinte sintaxe da macro:

```
@{notification_phrase[code].phrase}
```

código

Especifica o valor de Código único, como ConfidentialNotice, da tabela Message Phrases (usp_notification_phrase).

Observação: a tabela usp_notification_phrase lista as frases comuns que os modelos de mensagem de notificação podem usar. Para obter informações sobre a tabela usp_notification_phrase, consulte o *Guia de Referência Técnica*.

Por exemplo:

```
@{notification_phrase[IncidentURL1].phrase}
```

```
@{notification_phrase[RequestReply].phrase}
```

Quando o CA SDM localiza a macro, o texto da frase da tabela usp_notification_phrase substitui a sintaxe. Se não existe um código correspondente (ou se está inativo), uma sequência de caracteres vazia substitui a macro. Nenhum erro foi gravado para o log padrão (STDLOG), em vez disso, uma mensagem de aviso é registrada para ajudar a solucionar problemas em potencial.

Observação: a integração de frases em outras frases está limitada a um valor de profundidade máxima que você configura definindo a variável de ambiente (na página 382) NX_MAX_EXPAND_DEPTH. Essa limitação evita problemas que podem ocorrer ao processar frases que acidentalmente fazem referência a si mesmas (integram a si mesmas) ou fazem referência circular (quando uma frase integra uma frase em que está integrada).

Como frases de notificação aparecem em um exemplo de mensagem

Esse exemplo demonstra como as frases de notificação aparecem em uma mensagem de notificação. O exemplo usa os seguintes códigos e frases:

Código	Frase
ConfidentialNotice	Este email e quaisquer arquivos transmitidos com ele são para uso exclusivo do(s) destinatário(s) pretendido(s) e contêm informações que podem ser privilegiadas e confidenciais. Toda revisão, utilização, divulgação ou distribuição é proibida. Se você não é o destinatário pretendido deste email, por favor exclua este email e quaisquer arquivos transmitidos com ele e notifique o remetente imediatamente.
IncidentReply	Para adicionar um comentário ao seu incidente, basta responder a este email ou incluir a linha abaixo (em uma linha própria). %incident_id=@{call_req_id.ref_num}
IncidentURL	Clique no seguinte URL para exibir: @{call_req_id.web_url}

O seguinte modelo de mensagem inclui as frases de notificação:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} Fechado
Atribuído a: @{call_req_id.assignee.combo_name}
Cliente: @{call_req_id.customer.combo_name}
Descrição: @{call_req_id.description}

@{notification_phrase[IncidentURL].phrase}
@{notification_phrase[IncidentReply].phrase}

@{notification_phrase[ConfidentialNotice].phrase}
```

As frases aparecem em uma mensagem como segue:

```
Incidente 1234 fechado.
Atribuído a: analista, Joe
Cliente: Doe, John
Descrição: esta é uma descrição do meu problema

Clique no seguinte URL para exibir:
http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=40072
3
```

```
Para adicionar um comentário ao seu incidente, basta responder a este email ou incluir
a linha abaixo (em uma linha própria).
%incident_id=1234

Este email e quaisquer arquivos transmitidos com ele são para uso exclusivo do(s)
destinatário(s) pretendido(s) e contêm informações que podem ser privilegiadas e
confidenciais. Toda revisão, utilização, divulgação ou distribuição é proibida. Se
você não é o destinatário pretendido deste email, por favor exclua este email e
quaisquer arquivos transmitidos com ele e notifique o remetente imediatamente.
```

Lista de destinatários de notificação manual

É possível configurar um conjunto padrão de Destinatários disponíveis que a página de composição Notificação manual apresenta para solicitações, incidentes e problemas. Destinatários disponíveis simplificam o processo de notificação manual para analistas porque é possível configurar uma lista de objetos de contato (por exemplo, Usuário final afetado) ou nomes de contatos individuais para fácil uso como destinatários de notificações manuais.

Adicionar um Destinatário do contato de objeto adiciona os nomes de contatos individuais que o Contato de objeto representa para a lista Destinatários (consolidando quaisquer entradas duplicadas). O mesmo contato pode ser referido diversas vezes para diferentes Objetos de contato, como Responsável e Usuário final afetado. Algumas entradas, como o objeto de contato Lista de partes interessadas, podem adicionar diversas entradas à lista Destinatários.

Contatos e Objetos de contato permanecem na lista Destinatários disponíveis após adicioná-los à lista. Esse comportamento permite remover destinatários sem afetar a lista Destinatários disponíveis inicial.

Exemplo: como a lista Destinatários disponíveis funciona

Os exemplos a seguir demonstram como destinatários padrão simplificam o processo de notificação de atividade manual.

Destinatários do contato de objeto incluem as seguintes entradas:

- UserA pertence aos Objetos de contato "Responsável" e "Usuário final afetado".
- A Lista de partes interessadas inclui diversos nomes de contato. Por exemplo, UserB e UserC

Realize as seguintes ações:

- Adicione ambos os Objetos de contato que fazem referência ao UserA para a lista de Destinatários.

  Somente uma entrada do UserA é listada na lista Destinatários.

- Remova acidentalmente o UserA da lista Destinatários.

  Não é necessário fazer referência ao ticket para obter o nome do UserA e pesquisar para adicioná-lo de volta. É possível adicionar rapidamente o UserA à lista de Destinatários, pois o UserA é listado na lista de Destinatários disponíveis.

- Remova acidentalmente um nome de contato, como UserC, da lista Destinatários que veio da Lista de partes interessadas.

  É possível adicionar a Lista de partes interessadas a partir de Destinatários do contato de objeto para adicionar o nome do contato novamente. Uma vez que entradas duplicadas são consolidadas, outros Contatos na Lista de partes interessadas que não foram excluídos da lista Destinatários não são afetados.

Notificações para responsável anterior

Você pode definir configurar valores de Responsável ou Grupo anterior para uma notificação de atividade que detecta mudanças em campos chave quando um ticket for salvo. Valores anteriores permitem notificar um responsável anterior quando um ticket é transferido, ou notificar os grupos atual e anterior quando a prioridade de um ticket é encaminhada.

Os campos de valor Anterior de um ticket são campos locais que existem somente em memória, e não no banco de dados. Os campos são preenchidos durante a operação salvar de um ticket e apagados na conclusão do processamento da notificação. Um campo de valor anterior é associado com um tipo de atividade particular durante uma associação de atividade.

É possível definir valores Anteriores que detectem mudanças nos seguintes campos chave de um ticket:

Campo	Solicitações, Incidentes, Problemas	Requisições de mudança	Ocorrências
Status	Sim	Sim	Sim
Ativo	Sim	Sim	Sim

Campo	Solicitações, Incidentes, Problemas	Requisições de mudança	Ocorrências
Responsável	Sim	Sim	Sim
Área/Categoria da solicitação	Sim	Sim	Sim
Grupo	Sim	Sim	Sim
Impacto	Sim	Sim	Sim
Prioridade	Sim	Sim	Sim
Urgência	Sim	Não	Não
Gravidade	Sim	Não	Não

Existem vários contatos que você pode especificar para cada tipo de objeto (solicitação, incidente, problema, requisição de mudança ou ocorrência), que notificam os contatos atual e anterior quando uma atividade ocorre.

- **Responsável**—Pessoa atribuída para tratar o ticket.
- **Responsável anterior** — pessoa anteriormente atribuída para tratar o ticket.
- **Grupo** — grupo atribuído para tratar o ticket.
- **Grupo anterior** — grupo anteriormente atribuído para tratar o ticket.

Depois que a regra de notificação é salva, os campos Responsável anterior e Grupo anterior são exibidos na página de Lista de notificações de contato do objeto.

Por exemplo: configurar valores atual e anterior para campos chave

O seguinte exemplo de uso descreve como um administrador configura os valores atual e anterior dos campos chave, para garantir que o representante anterior do suporte seja notificado quando uma solicitação é transferida para outra pessoa.

1. **Situação —** um representante do suporte está frustrado porque um ticket foi transferido para outra pessoa e ele não foi notificado.
2. **Tarefa —** o administrador adiciona os contatos do objeto Responsável e Responsável anterior à regra de notificação para notificação da atividade de Transferência. Eles anexam um modelo de mensagem e especificam os responsáveis atual e anterior para notificar no formulário da solicitação.

3. **Ação —** quando a solicitação é salva, os campos Responsável e Responsável anterior da solicitação são preenchidos. Quando a atividade ocorre (o ticket é transferido), a condição para a regra é avaliada.
4. **Resultado —** se a condição for satisfeita, uma mensagem de notificação que descreve a atividade do ticket é enviada para o responsável atual e para o responsável anterior.

Exemplo de notificar contatos quando um ticket é transferido

Você pode notificar os contatos atual e anterior quando um ticket do CA SDM é transferido.

Exemplo: notificar tanto o contato atual quanto o anterior quando um ticket é transferido

1. Na guia Administração, vá para Notificações, Notificações de atividade.

   A página Lista de notificações de atividade aparece.

2. Selecione a notificação de atividade de transferência.

   A página Transfer Activity Notification Detail aparece.

3. No campo Tipo de objeto, selecione Solicitações/Incidentes/Problemas.
4. Na guia Regras de notificação, sob Símbolo, selecione Regra de notificação padrão de transferência.

   A página Regra de notificação padrão de transferência aparece.

5. Na guia Contatos de objeto, clique em Atualizar contatos de objeto.
6. Clique em Pesquisar.

   A página Notification Rule Update Recipients aparece.

7. Na lista Contatos do objeto, selecione Responsável e Responsável anterior na lista à esquerda e clique no botão de seleção de contato (>>).

   Os itens selecionados são adicionados à lista da direita.

   Observação: use as teclas CTRL ou SHIFT mais o botão esquerdo do mouse para selecionar vários contatos de objeto.

8. Clique em OK.
9. Salve a regra de notificação.

   A lista Contatos de objeto exibe o contato de objeto selecionado.

10. Na página Regra de notificação padrão de transferência, clique em Modelo de mensagem. Selecione um modelo e certifique-se de que a opção Notificação automática está ativada.

11. Crie uma solicitação, especifique um Responsável e clique em Salvar.
12. Na página Detalhes da solicitação, selecione Atividades e Transferência no menu Arquivo.
13. Especifique um novo Responsável e clique em Salvar.

    A notificação é enviada aos responsáveis atuais e anteriores quando ocorre uma atividade de transferência.

Notificações de item de configuração

Uma notificação de item de configuração (IC) permite definir uma notificação de atividade que esteja associada com um IC específico, que é associado com um ticket específico do CA SDM. Este recurso permite acompanhar informações sobre os usuários, organizações e fornecedores de um IC.

É possível especificar os contatos de objeto do IC na página Atualizar destinatários de regras de notificação, como Empresa mantenedora do IC, Contato primário do IC e assim por diante.

Notificar o contato principal de um item de configuração para um exemplo de ocorrência

É possível definir uma notificação de atividade para um contato principal que é enviada para um IC específico para um ticket específico do CA SDM.

Exemplo: notificar o contato principal de um item de configuração para uma ocorrência

1. Na guia Administração, vá para Notificações, Notificações de atividade.

   A página Lista de notificações de atividade aparece.
2. Selecione a notificação de atividade inicial na lista.

   A página Initial Activity Notification Detail aparece.
3. Selecione o tipo de objeto que deseja usar:
4. Na guia Regras de notificação, selecione o link Regra de notificação padrão.

   A página Default Notification Rule aparece.
5. Selecione o link Modelo de mensagem padrão e certifique-se de que a opção Notificação automática está ativada.
6. Selecione a guia Contatos de objeto e clique em Atualizar contatos de objeto.

   A página Pesquisa de notificação de contatos de objeto aparece.

7. Clique em Pesquisar. Uma lista de contatos de objeto aparece.
8. Selecione o Contato principal do IC na lista à esquerda e clique no botão de seleção de contatos (>>).

   Os itens selecionados são adicionados à lista da direita.

   Você pode usar as teclas CTRL ou SHIFT junto com o botão esquerdo do mouse para selecionar vários contatos de objeto. Você pode adicionar um objeto para uma solicitação e vários objetos para uma requisição de mudança ou ocorrência.

   Quando o contato de objeto está na lista à direita.
9. Clique em OK.
10. Salve a regra de notificação.

    A lista Contatos de objeto exibe o contato de objeto selecionado.
11. Execute as seguintes tarefas:
    - Na guia Service Desk, crie ou atualize um IC existente.
    - Adicione o contato principal listado na guia Contatos de objeto. O contato de objeto selecionado aparece na página Detalhes do item de configuração.
    - Adicione o IC à ocorrência.

Quando ocorre um evento de atividade, a regra é implementada e a condição é avaliada. Se os critérios para a condições forem alcançados, é enviada uma mensagem de notificação descrevendo a atividade do ticket é enviada a todos os contatos do IC associado a essa regra de notificação.

Notificações de pesquisa

Para uma notificação de atividade, é possível definir detalhes de notificação de pesquisa separados para tickets, pesquisas gerenciadas, documentos de conhecimento e comentários de conhecimento e enviá-la para o cliente que iniciou a atividade.

Usando notificações de pesquisa, é possível:

- Especificar uma nova pesquisa ou usar uma das pesquisas padrão disponíveis no produto.
- Usar métodos de notificação que descrevem como as mensagens de notificação são enviadas aos usuários.
- Definir uma mensagem de pesquisa para o cliente.

Quando um usuário recebe uma notificação de pesquisa, o corpo da mensagem automaticamente inclui um URL que pode ser acessado em um navegador da Web para localizar e preencher o formulário de pesquisa.

Um log de atividades é gerado quando uma notificação de pesquisa é enviada e quando é recebida de volta de um cliente.

Mais informações:

Definir notificações de pesquisa (na página 211)

Como adicionar hiperlinks de URL a notificações

O campo web_url das tabelas Change_Request e workflow_Task contém um valor de URL que permite um usuário acessar uma requisição de mudança ou tarefa de fluxo de trabalho determinada por meio da interface web. Quando usado em notificações de email, um usuário pode clicar no URL e ir à interface web sem qualquer outra consulta.

Para implementar hiperlinks de URL em notificações, configure seu sistema como segue:

1. Instale e configure a interface web de CA SDM.

   Observação: para obter mais informações sobre como configurar a interface web no CA SDM, consulte o *Guia de Implementação*.

2. Usando o Gerenciador de opções, configure e instale a opção web_cgi_url para especificar o local do mecanismo da web do CA SDM, por exemplo, http://hostname/scripts/pdmcgi.exe.

Mais informações:

Uso do Gerenciador de opções (na página 381)

Leitor de logs de notificação

O Leitor de logs de notificação exibe as notificações recebidas para o usuário conectado de acordo com sua data, urgência e status. Com o Leitor de logs de notificação, é possível fazer o seguinte:

- Alterar a ordem de classificação e definir opções de menu para que o Leitor de logs de notificação seja exibido automaticamente quando novas mensagens forem recebidas.
- Clicar duas vezes em uma mensagem de notificação para solicitar que o CA SDM exiba a página de detalhes para o ticket associado com a notificação.
- Monitorar mensagens de notificação inserindo os critérios específicos de seleção para consulta ao banco de dados a fim de analisar ou selecionar mensagens de notificação com base em dados inseridos nos campos. Por exemplo, você pode listar apenas as mensagens de notificação que não foram limpas alterando o campo Status da mensagem para Não limpa.
- Limpar mensagens de notificação para manter sua lista de notificações com um tamanho gerenciável. As notificações limpas não são exibidas quando você acessa o Leitor de logs de notificação, embora você possa escolher exibi-las, se necessário.

Configurar as Opções do Leitor de logs de notificação

Você pode definir opções para o Leitor de logs de notificação para definir como será notificado quando novas mensagens forem recebidas para uma ocorrência.

Para configurar opções para o Leitor de logs de notificação

1. Na guia Service Desk, navegue para Exibir, Leitor de logs.

   A página Leitor de logs de notificação é exibida.

2. Use a caixa de seleção à esquerda de cada notificação para configurar as seguintes opções. Você pode selecionar itens para executar operações como Limpar selecionados ou Excluir selecionados.

   Cabeçalho

   Mostra o cabeçalho da mensagem, que normalmente contém o número do ticket e o tipo de atividade.

   Data de início

   Exibe a data e a hora em que a notificação foi enviada à sua janela Leitor de logs.

Status

Exibe o status da notificação.

Urgência

Define o nível de urgência da notificação (baixa, alta, normal ou emergência), que indica a importância relativa de atividades diferentes. Os níveis de urgência são predefinidos; no entanto, o administrador do sistema é responsável por configurar outros aspectos da notificação, tais como métodos de notificação e associações de atividade. O administrador do sistema também define o método de notificação usado para contatos e grupos para cada nível de urgência.

Texto da mensagem

O texto completo da mensagem de notificação.

O Leitor de logs exibe as mudanças.

3. Clique em Fechar.

   A página Leitor de logs de notificação fecha e as opções são definidas.

Respostas personalizadas

Você pode criar respostas personalizadas e anexá-las a solicitações, ocorrências e registros da requisição de mudança quando adiciona atividades ao registro. Você pode, por exemplo, acrescentar respostas personalizadas nas janelas Mudança de status ou Registrar comentários disponíveis no menu Atividades.

Criar uma resposta personalizada

É possível criar uma resposta personalizada para anexar a registros de solicitações, ocorrências e requisição de mudança.

Para criar uma resposta personalizada

1. Na guia Administração, navegue para Service Desk, Respostas personalizadas.

   A página da lista Respostas personalizadas aparece.

2. Clique em Criar novo.

   A página Criar nova resposta personalizada aparece.

3. Preencha os campos na página.

   Proprietário da resposta

   Especifica o contato que é proprietário da resposta. Se este campo for deixado em branco, a resposta estará disponível a todos os analistas.

   Resposta

   Especifica o texto entregue a todos os que recebem esta resposta. Esse campo pode ser de até 1000 caracteres.

   Você pode usar variáveis nesse campo, por exemplo:

   ```
   Ticket ref_num: @{call_req_id.ref_num}
   Destinatário: @{call_req_id.assignee.combo_name}
   Cliente: @{call_req_id.customer.combo_name}
   Descrição: @{call_req_id.description}
   ```

4. Selecione o tipo de registro para o qual você quer disponibilizar esta resposta. Clique em Salvar.

   Uma resposta personalizada é criada.

Substituição de variável de resposta personalizada

As variáveis podem ser incorporadas ao texto de uma Resposta pessoal. Essas variáveis permitem que as informações sejam substituídas da solicitação, requisição de mudança, ocorrência, problema ou incidente correspondente. A sintaxe das variáveis é a mesma usada em qualquer outra parte no produto CA SDM, como nos modelos de mensagem de notificação de atividade e em Notificar manualmente texto da mensagem de atividade. As informações só podem ser substituídas da solicitação, requisição de mudança, ocorrência, problema ou incidente correspondente. Os modelos de mensagem de notificação de atividade e Notificar manualmente texto da mensagem de atividade permitem que as informações do registro de log de atividades sejam incluídas também.

As caixas de seleção para cada tipo de objeto (Solicitações, Requisições de mudança, Ocorrências, Incidentes e Problemas) permitem que as respostas sejam filtradas durante a seleção. Se o tipo de objeto não for selecionado, a Resposta não estará disponível para esse objeto. Por exemplo, se somente a caixa Solicitação estiver marcada, a Resposta somente será apresentada em Atividades para uma Solicitação.

Uma única resposta pode ser usada para todos os tipos de objeto (Solicitações, Requisições de mudança, Ocorrências, Problemas ou Incidentes). Como cada objeto tem diferentes atributos, informações que não se apliquem ao objeto não são substituídas (por exemplo, a tentativa de substituir o Número da solicitação em uma Resposta para uma ocorrência.

Abaixo está um exemplo de texto de Resposta e as substituições de variáveis que ocorrem para cada tipo de objeto:

```
Este é o nº da solicitação '@{call_req_id.ref_num}'
Este é o nº da requisição de mudança '@{change_id.chg_ref_num}'
Este é o nº da ocorrência '@{issue_id.ref_num}'
```

Para uma *Solicitação*, a seguinte substituição ocorre:

```
Este é o nº da solicitação 'cr_demo:11'
Este é o nº da requisição de mudança"
Este é o nº  da ocorrência"
```

Para uma *Requisição de mudança*, a seguinte substituição ocorre:

```
Este é o nº da solicitação"
Este é o nº da requisição de mudança 'chg_demo:3'
Este é o nº  da ocorrência"
```

Para uma *Ocorrência*, a seguinte substituição ocorre:

```
Este é o nº da solicitação"
Este é o nº da requisição de mudança"
Este é o nº da ocorrência 'iss_demo:6'
```

Ao utilizar as caixas de seleção "Exibir esta resposta para", versões diferentes de uma Resposta podem ser criadas com as variáveis de substituição apropriadas para o objeto correspondente (Solicitações, Requisições de mudança, Ocorrências, Problemas ou Incidentes).

O formato das variáveis de substituição para os objetos diferentes é como se segue.

Objeto	Formato da variável
Solicitação / Incidente / Problema	@{call_req_id.attr}
Requisição de mudança	@{change_id.attr}
Ocorrência	@{issue_id.attr}

A substituição ocorre quando a Resposta é copiada para o campo Descrição do usuário. A Resposta é copiada depois de ser selecionada no menu suspenso Resposta personalizada e de o menu suspenso perder o foco.

Administração de email

O email permite a comunicação com usuários finais, como funcionários ou clientes. Usuários finais podem responder a notificações de email para atualizar ou criar tickets usando email a partir de um computador ou de outro dispositivo, como um telefone celular ou smartphone. Por exemplo, uma resposta a uma notificação de email enviada a um usuário final para obter informações adicionais pode atualizar um ticket com as informações solicitadas.

Os seguintes recursos processam a comunicação de email de e para o usuário final:

- **Notificações por email** — processa emails de saída.

  Considere as seguintes informações sobre emails de saída:

  - O daemon de correio (pdm_mail_nxd) envia notificações de correio de saída usando Simple Mail Transfer Protocol (SMTP).
  - Você configura as opções de SMPT do servidor de correio usando o Gerenciador de opções, Email.
  - É possível usar métodos de notificação por email padrão (ou configurar novos métodos) para enviar correios diretamente ao destinatário através do correio SMTP.

- **Caixas de correio** — processam emails de entrada.

  Considere as seguintes informações sobre emails de entrada:

  - O Mail Eater (pdm_maileater_nxd) recupera emails de entrada para criação e atualizações de tickets usando o Post Office Protocol (POP3) ou o Internet Message Access Protocol (IMAP ou IMAP4).
  - As caixas de correio do CA SDM definem contas de email (caixas de entrada).
  - Regras de caixa de correio definem como cada caixa de correio processa correios de entrada.

Mais informações:

Notificações de email (na página 109)

Caixas de correio

O CA SDM fornece uma caixa de correio padrão que se conecta ao servidor de correio e que requer configuração adicional, como definir valores para nome de host, nome de usuário, senha e assim por diante.

Algumas das maneiras que você pode definir uma caixa de correio para processar correio de entrada são:

- Configurar uma caixa de correio para usar protocolo IMAP ou POP3.
- Criar diversas caixas de correio para permitir que inquilinos individuais ou organizações tenham diferentes caixas de correio, com comportamentos separados para cada uma.
- Usar regras da caixa de correio para filtrar mensagens e definir comportamento específico, definir respostas automáticas e definir ações específicas (por exemplo, atualizar tickets), com base nos conteúdos ou propriedades da mensagem.
- Use regras da caixa de correio para fornecer padrões de API de texto e estabelecer interfaces de email com outro software. É possível configurar parâmetros (como categoria, responsável, e assim por diante) especificamente para a interface.
- Use frases de notificação nas regras da caixa de correio para criar elementos comuns para respostas automáticas em diversas regras.
- Use políticas da caixa de correio para ajudar a proteger contra abuso com base em correio.

Mais informações:

Polling de caixa de correio (na página 112)

Regras de caixa de correio

As regras da caixa de correio permitem configurar quaisquer ações, respostas, ou ambas, que devem ocorrer para mensagens recuperadas de uma caixa de correio. A tabela (usp_mailbox_rule) mantém as regras que se aplicam à conexão para cada conta de servidor de correio (usp_mailbox); as regras pertencem a caixas de correio específicas. Você pode excluir regras ou torná-las inativas para desativá-la.

Observação: ao criar as regras da caixa de correio, você as associa a uma caixa de correio específica—outra caixa de correio não pode compartilhar essas regras. Se desejar usar regras que pertencem a uma caixa de correio para uma caixa de correio diferente, recrie-as para a outra caixa de correio.

As regras da caixa de correio permitem também fazer o seguinte:

- Especificar diversos comportamentos para mensagens de cada caixa de correio com base nos conteúdos das mensagens.
- Fornecer parâmetros padrão da API de texto (como categoria, responsável e assim por diante) para o processamento e roteamento de mensagens.
- Definir filtros de mensagem com base em expressões regulares ou palavras-chave fixas.
- Use uma frase de notificação comum para respostas automáticas para diversas definições das regras da caixa de correio, como no exemplo a seguir:

  ```
  Obrigado por enviar sua solicitação.
  @{notification_phrase[RequestReply].phrase}
  ```

  A frase aparece em respostas a email entregue a quaisquer caixas de correio que incluam a regra.

Mais informações:

Ações de regra de caixa de correio (na página 146)
Coincidência de padrão em regras de caixa de correio (na página 147)
Restrições de identificador de objeto de sequência de caracteres de filtro (na página 149)
Caracteres especiais em expressões comuns (na página 151)
Exemplo de texto para frases de notificação em uma regra de caixa de correio (na página 152)
Como criar uma regra de caixa de correio que corresponda a cada mensagem recebida (na página 152)
Como usar as configurações de Padrões TextAPI das regras da caixa de correio e de TextAPI Ignore Incoming. (na página 153)

Ações de regra de caixa de correio

Regras da caixa de correio permitem realizar qualquer das seguintes ações de email:

- Ignorar email — não processa o email e não responde.

  Essa ação é útil para mensagens de nível de sistema, como erros Out of Office ou Mail Delivery.

- Ignorar email e a resposta — não processa o email e responde ao remetente. Emails de resposta usam as mensagens de sucesso na resposta e mensagens de falha na resposta são ignoradas.

- Atualizar objeto — usa a sequência de caracteres de filtro para determinar o identificador do objeto (por exemplo, %Incident:{{object_id}}% no email) e envia uma solicitação de atualização à API de texto. Se o identificador do objeto não for encontrado, a API de texto não realiza nenhuma ação.

  Essa ação tipicamente trata respostas de email em que o identificador de objeto está integrado no email. Se nenhum identificador de objeto estiver presente, a mensagem de falha na resposta geralmente é enviada.

- Criar/atualizar objeto — usa a sequência de caracteres de filtro para determinar o identificador do objeto (por exemplo, %Incident:{{object_id}}% no email) e envia uma solicitação de atualização à API de texto. Se o identificador do objeto for encontrado, a API de texto atualiza um ticket.. Se o identificador do objeto não for encontrado, a API de texto cria um ticket..

  Essa ação é o comportamento padrão do daemon de correio (Mail Eater) no qual o email contém ou não contém palavras-chave da API de texto.

Observação: para obter informações sobre as regras de configuração da caixa de correio, consulte a *Ajuda online*.

Coincidência de padrão em regras de caixa de correio

Regras de caixa de correio usam expressões comuns para a correspondência de padrões. Considere os seguintes caracteres de espaço em branco que se aplicam a expressões comuns em regras de caixa de correio:

\t

Especifica uma guia horizontal.

****

Especifica um caractere de retorno de linha.

\n

Especifica um caractere de nova linha.

Os caracteres que representam quebras de linha em texto podem variar com o sistema operacional, servidor de correio e cliente de correio, por exemplo:

- UNIX usa um \n.
- Microsoft usa \r\n
- Macintosh usa \r
- MacOS X usa \n

Em certas circunstâncias, os elementos de processamento de correio do CA SDM trocam ou substituem um destes caracteres de quebra de linha por outro para estabelecer ou manter uma distinção entre diferentes elementos de texto, como texto da mensagem e parâmetros anexados. Como resultado, quando quiser usar uma quebra de linha ou parágrafo, crie seus filtros de forma que tanto \r quanto \n possam ser correspondidos, seja qual for deles que for encontrado. Se quiser indicar uma quebra de linha entre duas palavras-chave, crie seus filtros para que uma sequência de um ou mais caracteres \r e \n possam ser correspondidos.

A quebra de linha pelo cliente de correio que envia a mensagem pode causar quebras de linhas inesperadas aparecendo no meio do texto que deveria corresponder à sequência de caracteres de seu filtro quando ele procura no corpo da mensagem. Um espaço pode ser modificado para um retorno de linha, nova linha ou ambos, ou qualquer um deles pode ser inserido depois de um espaço. Se uma mensagem foi composta em HTML, e contém listas numeradas ou com indicadores, ou parágrafos recuados, as tabulações também podem estar presente depois que o cliente de correio converte e envia a mensagem. Ao incluir espaços no meio de uma sequência de caracteres do filtro, use um bloco de Expressão comum que represente qualquer espaço em branco de tamanho variável. Esse bloco é [\t\r\n]+ (colchete, espaço, barra invertida, t, barra invertida, r, barra invertida, n, colchete, sinal de mais), e representa qualquer sequência de um ou mais espaços, tabulações, retornos de linha e novas linhas.

Exemplo: usar [\t\r\n] para corresponder exatamente a uma palavra-chave

Este exemplo demonstra como usar caracteres de espaço em branco para corresponder à palavra-chave "request" e não corresponder a nenhuma outra palavra-chave possível, como as palavras seguintes:

```
requester
requesting
requested
orequestra
```

Para corresponder somente à palavra-chave "request", coloque, antes e depois, um ou mais caracteres de espaço em branco conforme abaixo:

```
[ \t\r\n]request[ \t\r\n]
```

O Mail Eater corresponde somente à palavra "request" ou a palavra como parte de uma frase, e não como parte de outra palavra, como "requester".

Restrições de identificador de objeto de sequência de caracteres de filtro

Aplicam-se restrições a sequências de caracteres de filtro da regra da caixa de correio que determinam o identificador do objeto (por exemplo, %Incident:{{object_id}}%) em um email. O texto que envolve um identificador de objeto ({{object_id}}) deve ser não ambíguo tanto em conteúdo quanto em comprimento; o texto deve definir claramente o início e o final do valor de objeto da ID do ticket que está entre o texto.

As seguintes restrições se aplicam a como o Mail Eater interpreta o *início* do valor de objeto da ID do ticket:

- O espaço reservador {{object_id}} não deve ser o primeiro elemento na sequência de caracteres de filtro. Pelo menos um caractere é necessário, e geralmente uma palavra-chave distinta, ou uma sequência de letras, números e símbolos deve preceder a palavra-chave da ID do objeto.
- O caractere que precede imediatamente o espaço reservado {{object_id}} não deve ser um caractere repetível ou opcional (ou seja, um caractere seguido por um sinal de mais (+), um asterisco (*) ou um ponto de interrogação (?)) que pode ser parte de um valor de objeto da ID do ticket. Caracteres repetíveis ou opcionais correm o risco de serem ambíguos com o início do valor de objeto da ID do ticket, a menos que sejam caracteres de espaço em branco. Os caracteres de espaço em branco (espaço, tabulação, retorno de carro, avanço de linha) não devem fazer parte do valor de um artefato da ID de ticket.
- O caractere que precede imediatamente o espaço reservado {{object_id}} não deve ser um conjunto entre colchetes repetível ou opcional de caracteres, o que inclui caracteres que podem ser parte de um valor de Objeto da ID do Ticket.

As seguintes restrições se aplicam a como o Mail Eater interpreta o *comprimento* do valor de objeto da ID do ticket:

- O espaço reservador {{object_id}} não deve ser o último elemento em uma Sequência de caracteres de filtro. Um ou mais caracteres devem seguir o espaço reservado {{object_id}}.
- O caractere que segue imediatamente o espaço reservado {{object_id}} não deve ser um caractere repetível ou opcional (ou seja, um caractere seguido por um sinal de mais (+), um asterisco (*) ou um ponto de interrogação (?)) que pode ser parte de um valor de objeto da ID do ticket. Caracteres repetíveis ou opcionais correm o risco de serem ambíguos com o final do valor de objeto da ID do ticket, a menos que sejam caracteres de espaço em branco. Os caracteres de espaço em branco (espaço, tabulação, retorno de carro, avanço de linha) não devem fazer parte do valor de um artefato da ID de ticket.
- O primeiro caractere após o espaço reservado {{object_id}} não deve ser um caractere que possa ser parte de um valor de objeto da ID do ticket.
- Evite os seguintes caracteres imediatamente antes e após o espaço reservado {{object_id}}:
  - Todas as letras em maiúsculas ou todas em minúsculas
  - Numerais
  - O sinal de mais (+)
  - A barra (/)
  - A vírgula (,)
  - O ponto (.), porque pode representar qualquer caractere, exceto uma quebra de linha, e, portanto, pode ser qualquer um dos caracteres nesta lista.

  porque qualquer desses caracteres pode existir no valor de objeto da ID do ticket. Quando um conjunto entre colchetes (diversos caracteres entre colchetes, dos quais a verificação de filtro pode combinar qualquer um), precede ou segue o espaço reservado {{object_id}}, o conjunto entre colchetes não deve conter nenhum desses caracteres.

Caracteres especiais em expressões comuns

Combinação de padrão para os filtros nas regras da caixa de correio seguem as regras para Expressões Regulares ASCII com caracteres especiais estilo C.

Importante: Recomendamos que você esteja familiarizado com a sintaxe Regex para usar caracteres especiais em expressões regulares.

Por exemplo, considere os seguintes caracteres especiais para padrões Regex que se aplicam a expressões regulares nas regras da caixa de correio:

\t

Especifica uma guia horizontal. Nas sequências de caracteres de filtro para as regras da caixa de correio, \t combina o início e o final do texto (e guias) e é específico para o Mail Eater.

****

Especifica um retorno de linha (retorno ao começo da linha atual).

Observação: não use \r para pesquisar assuntos de mensagem ou enviar endereços.

\n

Especifica uma nova linha (combinação de feed de linha e retorno de linha).

Observação: não use \n para pesquisar assuntos de mensagem ou enviar endereços.

\t, \r e \n são caracteres especiais que ocorrem com mais frequência em expressões regulares para as regras da caixa de correio.

Exemplo: uso de \t, \r, e \n

```
[ \t]solicitação[ \t]
```

Pesquisa texto para a palavra solicitação. Os colchetes combinam qualquer caractere do conjunto, incluindo o espaço, então [\t] combina um espaço ou uma tabulação.

```
[\r\n]+crítico[ \t\r\n]
```

Pesquisa texto para a palavra crucial no começo de uma linha, começo da mensagem ou todos os conteúdos de uma linha. Os colchetes combinam qualquer caractere do conjunto e o + (sinal de mais) combina um ou mais dos anteriores, então [\r\n]+ combina um ou mais retornos de linha e novas linhas.

Exemplo de texto para frases de notificação em uma regra de caixa de correio

Este exemplo mostra texto que você pode usar para incluir frases de notificação em uma regra da caixa de correio. Você pode definir versões separadas de uma frase de notificação para texto sem formatação e para HTML quando a frase contém quaisquer quebras de linha ou outra formatação.

Use o texto a seguir no campo Texto de êxito, HTML de êxito ou ambos os campos na página Atualizar regra da caixa de correio, guia Resposta bem-sucedida:

- Texto de êxito

```
Obrigado por enviar sua solicitação.
@{notification_phrase[IncidentURL1].phrase}
```

- HTML de êxito

```
Obrigado por enviar sua solicitação.</p>
@{notification_phrase[IncidentURL1H].phrase}</p>
```

Observação: para obter mais informações sobre as Frases de notificação definidas na guia Administração, Notificações, Frases de notificação, consulte a *Ajuda online*.

Mais informações:

Sintaxe de frase de notificação (na página 130)
Códigos e frases de notificações (na página 128)

Como criar uma regra de caixa de correio que corresponda a cada mensagem recebida

É possível criar uma regra de caixa de correio que corresponda a cada mensagem recebida que outra regra de caixa de correio não filtra.

Para criar esse tipo de regra, defina o filtro como O assunto contém e a sequência de caracteres de filtro como um ponto e um asterisco (".*").

- Um ponto corresponde a qualquer caractere, exceto a quebra de linha.
- Um asterisco corresponde a zero ou mais ocorrências do símbolo imediatamente antes dele.

Como resultado, essa combinação corresponde a zero ou mais caracteres que não são quebras de linha.

Exemplo: uma regra de caixa de correio "Catch-All"

Esse exemplo demonstra como é possível usar um combinação ".*" para corresponder a cada mensagem recebida:

```
Filtro = "O assunto contém"
Sequência de caracteres de filtro = ".*"
```

Como usar as configurações de Padrões TextAPI das regras da caixa de correio e de TextAPI Ignore Incoming.

Os campos Padrões TextAPI e TextAPI Ignore Incoming permitem especificar valores padrão para regras de caixa de correio de entrada e especificar comandos da TextAPI que não devem ser aceitos em emails recebidos. Esses campos funcionam com os valores padrão definidos na seção [EMAIL_DEFAULTS] e com a lista de comandos proibidos na seção [EMAIL_IGNORE_INCOMING] do arquivo text_api.cfg. Quando ocorre um conflito entre a definição em uma regra de caixa de correio e a definição no arquivo text_api.cfg, o valor definido na regra de caixa de correio se aplica.

O campo Padrões TextAPI inclui os comandos de palavra-chave TextAPI que são aplicados a um ticket quando é criado a partir de um email que corresponde a uma regra de caixa de correio. Os comandos não são aplicados quando a mensagem afeta um ticket existente.

Para especificar comandos Padrões TextAPI, faça o seguinte:

1. Coloque cada comando em uma linha separada no campo Padrões TextAPI.
2. Formate os comandos como segue:

   `OBJECT.FIELD=`*`value`*

   Observação: não inclua um símbolo de porcentagem inicial (%), que é necessário somente para comandos correspondentes integrados no corpo do email.

   Por exemplo, formate os comandos como segue:

   ```
   REQUEST.PRIORITY=3
   PROBLEM.CATEGORY=Facilities
   INCIDENT.GROUP=Plumbing
   ```

O campo TextAPI Ignore Incoming lista os comandos da palavra-chave TextAPI que não têm permissão para serem usados no texto da mensagem de email recebida. Quaisquer comandos relacionados nesse campo são ignorados quando são encontrados em uma mensagem de email recebida.

Para especificar comandos TextAPI Ignore Incoming, faça o seguinte:

1. Coloque cada comando em uma linha separada no campo TextAPI Ignore Incoming.
2. Formate os comandos como segue:

   ```
   OBJECT.FIELD
   ```

   Observação: não inclua um símbolo de percentagem inicial (%), que é necessário somente para comandos correspondentes integrados no corpo do email.

   Por exemplo, formate os comandos como segue:

   ```
   CHANGE.ASSIGNEE
   PROBLEM.GROUP
   REQUEST.EFFORT
   ```

3. Defina todos os comandos usados em cada campo na seção [KEYWORDS] do arquivo text_api.cfg. Esse arquivo é localizado no subdiretório "local" do diretório de instalação do CA SDM.

Políticas de caixa de correio

Políticas da caixa de correio protegem a organização contra certos tipos de abuso de email. É possível implementar políticas das seguintes maneiras:

- É possível definir listas de inclusão e exclusão de endereços de email:
  - Listas de inclusão limitam o recebimento de email apenas para o correio enviado de determinados endereços de email (por exemplo, user@company.com) ou domínios de email (por exemplo, company.com) em particular.
  - Listas de exclusão que organizam endereços ou domínios de email indesejados.

A lista de inclusão padrão para cada caixa de correio é um asterisco (*). Um asterisco em si como um nome inteiro nesta lista especifica World Domain, e representa todos os domínios de email não inclusos na lista de exclusão. Essa representação evita ambiguidade quanto a se a lista de inclusão é a lista completa de domínios permitidos ou as exceções aos domínios na lista de exclusão como segue:

- Uma lista de inclusão que inclui World Domain especifica que todas as outras entradas na lista de inclusão são exceções à lista de exclusão, e apenas domínios ou endereços na lista de exclusão são bloqueados (com a exceção dos endereços específicos na lista de inclusão).

- Uma lista de inclusão que não contém World Domain especifica que somente endereços e domínios listados na lista de inclusão têm permissão para postar, e somente se o domínio (se o endereço específico não estiver na lista de inclusão) ou endereço do remetente não estiver na lista de exclusão.

- É possível definir o limite Maximum Messages Per Hour Per Address para detecção de DoS (Denial of Service, Negação de Serviço).

  Maximum Messages limita o número de emails por hora que qualquer endereço de email tem permissão para enviar para aquela caixa de correio. Se um endereço de email ultrapassar o limite, ele é adicionado à lista de exclusão. Mais nenhuma mensagem desse endereço de email do remetente é processada para essa caixa de correio até que você remova o endereço de email da lista de exclusão.

  As políticas da caixa de correio para listas de inclusão e exclusão e o número máximo de emails permitido por hora referem-se apenas àquela caixa de correio associada. Um endereço adicionado automaticamente para uma lista de exclusão de caixa de correio por violar a restrição de número máximo de emails não é adicionado automaticamente à lista de exclusão para nenhuma outra caixa de correio, o mesmo acontece com a conta de email usada para outras caixas de correio.

Endereços de email que violem a política são registrados no STDLOG com base nas configurações de log_policy_violation (Nenhum, Log First ou Log All).

Como implementar caixas de correio

O CA SDM fornece uma caixa de correio (chamada Padrão) que está ativa e pode ser usada na organização. Você pode modificar a caixa de correio padrão, criar caixas de correio adicionais ou ambos.

Para implementar caixas de correio, siga as seguintes etapas preliminares:

- Configure a conta de servidor de correio que deseja usar.
- Crie contatos e especifique seus endereços de email se não deseja permitir que usuários anônimos criem e atualizem tickets (opção Permitir anônimo).

Para configurar a caixa de correio Padrão, siga as seguintes etapas opcionais básicas:

1. Editar a caixa de correio padrão.
2. Atualizar as regras e as políticas da caixa de correio conforme o adequado.

   A caixa de correio está ativa e começa a sondagem. A primeira consulta ocorre após um segundo.

Configurar o servidor de correio

Notificações para um evento (notificação automática e manual) são enviadas usando uma única definição de servidor de correio.

Para configurar o servidor de correio

1. Na guia Administração, navegue para Gerenciador de opções, Email.

   A página Lista de opções aparece.

2. Clique na opção que deseja instalar.

   A página Detalhes de opções aparece.

3. Clique em Editar, preencha os campos como adequado e clique em Instalar.

   O servidor de corredio é configurado para enviar notificações (correio de saída).

4. Repita o procedimento até que todas as opções da Lista de opções relevantes estejam configuradas.

Observação: é possível usar os parâmetros -F e -T do comando pdm_mail, que define o Remetente e o endereço Responder a, respectivamente. Usando esses parâmetros em métodos de notificação personalizados, as respostas a notificações de correio recebido podem ser direcionadas para a caixa de correio adequada.

Mais informações:

Utilitário pdm_mail - Enviar notificação de email (na página 107)

Opções de email

A interface de email envia notificações de email e permite que os usuários criem tickets a partir de um email. As opções de email permitem configurar os protocolos de correio de saída.

mail_from_address

Especifica a notificação de correio do endereço De: O endereço está no formato Displayname<user@company.com>.

mail_login_password

Especifica a senha de logon do servidor SMTP.

mail_login_userid

Especifica a ID de usuário para logon do servidor SMTP.

mail_max_threads

Especifica o número máximo de conexões simultâneas de SMTP que podem tentar se comunicar com o servidor.

mail_reply_to_address

Define a resposta para endereços para notificação de email. Essa opção é útil se os emails forem enviados de uma conta de usuário, mas desejar que as respostas sejam enviadas a outro endereço de email. O valor padrão é o mesmo do endereço "de".

mail_smtp_domain_name

Define o nome de domínio que é exigido por alguns servidores SMTP que entendem os protocolos ESMTP. É possível limpar o nome de domínio ao definir o valor para NONE.

mail_smtp_hosts

Especifica uma lista separada por espaço de nomes de host SMTP para notificações de email.

mail_smtp_host_port

Especifica uma porta SMTP para substituir a porta STMP padrão.

mail_smtp_security_level

Especifica o nível de segurança SMTP. As configurações válidas são: 0=no security, 1=basic authentication, 2=NTLM, 3=MD5 e 4=LOGIN. Se definir esta opção para 1, defina as opções mail_login_password e mail_login_userid. A maioria dos servidores STMP não exige autenticação.

Editar a caixa de correio padrão

O CA SDM fornece uma caixa de correio ativa padrão que pode ser editada para corresponder às necessidades de entrega de correio da organização.

Para editar a caixa de correio padrão

1. Na guia Administração, acesse Email, Caixas de correio.

   A Lista de caixas de correio é exibida e lista as caixas de correio ativas.

2. Clique em Padrão na coluna Nome.

   A página Detalhes da caixa de correio padrão é exibida.

3. Clique em Editar.
4. Complete ou atualize os outros campos conforme o adequado:

   Sequência

   Especifica o número de sequência da resposta. As mensagens são verificadas contra as regras em ordem do número de sequência do menor até o maior.

   Caixa de correio

   Especifica a caixa de correio à qual esta regra pertence.

   Ativo

   Define a regra como ativa ou inativa.

   Filtrar

   Especifica qual parte do e-mail pesquisar pelo padrão do filtro, por exemplo, Assunto contém.

   Sequência de caracteres de filtro

   Especifica uma sequência de expressão regular para corresponder, por exemplo, a [\t\r\n]request[\t\r\n]. O espaço reservado {{object_id}} permite especificar o valor do artefato do Texto API para usar para associar a mensagem ao ticket específico.

Ignorar caso

Especifica a consideração de letras maiúsculas ou minúsculas ao fazer a correspondência de padrões.

Ação

Especifica a ação a tomar quando correspondem os critérios de filtro, por exemplo, Criar/Atualizar Objeto.

Observação: para informações sobre ações de regra, consulte a *guia administração*.

Objeto de ação

Exibe o tipo de objeto de ticket ao qual se aplicam as ações de mensagem, por exemplo, Solicitação.

Tipo de artefato mínimo

Define o tipo mínimo de verificação de artefato que você deseja permitir:

- **NONE -** especifica nenhuma validação de artefatos Este valor é o mesmo que não adicionar a palavra-chave ao arquivo de entrada. Também aceita comandos da ID de ticket de Texto API.
- **PROTECTED** — valida um ticket contra o hash de confirmação. Se a confirmação falhar, o artefato é considerado inválido e o email falha a filtragem quando a filtragem estiver pesquisando um artefato ({{object_id}}).
- **SECURE** — valida o número do ticket a partir de um bloco de dados criptografados. Se o valor não for um número de ticket criptografado válido, o artefato é considerado inválido e o email falha a filtragem quando a filtragem estiver pesquisando um artefato ({{object_id}}).

Observação: os tipos que forem mais seguros do que os definidos são permitidos. Em outras palavras, se você definir o tipo mínimo como PROTECTED, então são permitidos tanto PROTECTED quanto SECURE, porém NONE não é permitido. Do mesmo modo, se PROTECTED ou SECURE estiverem selecionados, os comandos da ID de ticket do Texto API não são aceitos.

Responder

Especifica um método de notificação para enviar uma resposta automática, por exemplo, Email. Se você não definir esta opção, não será retornada nenhuma resposta. A resposta indica êxito ou falha das ações realizadas para a mensagem, e é separada de quaisquer notificações.

Assunto -

Especifica uma linha de assunto para a resposta, por exemplo, resposta do Service Desk.

Gravar em stdlog

Gravar texto de email no log padrão (stdlog) se o filtro corresponder.

Log Entry Prefix

Especifica um prefixo para adicionar ao gravar texto de email nas entradas de log padrão. Use esta opção para ativar a correspondência de entradas de log às regras.

Add Subject Line

Adiciona a linha assunto da mensagem original ao corpo da mensagem antes do processamento. É possível acrescentar, pré-anexar ou não adicionar uma linha de assunto. A linha assunto está vinculada à descrição do ticket ou um comentário de log, dependendo das ações da mensagem.

Padrões de Texto API

Especifica comandos padrão adicionais para a API de texto quando o filtro corresponder.Combinado com o conteúdo da seção [EMAIL_DEFAULTS] do arquivo text_api.cfg.

Texto API Ignorar recebido

Especifica detalhes adicionais a ignorar para a API de texto quando o filtro corresponder.Combinado com o conteúdo da seção [EMAIL_IGNORE_INCOMING] do arquivo text_api.cfg.

Detalhes

Especifica informações sobre a regra.

Texto de êxito

Especifica o conteúdo de texto sem formatação de uma mensagem de resposta quando a mensagem for processada com êxito. Por exemplo:

```
Obrigado por enviar uma atualização à sua solicitação. Um técnico de suporte
entrará em contato com você nas próximas 24 horas.
```

HTML de êxito

Especifica o conteúdo HTML de uma mensagem de resposta quando a mensagem é processada com êxito. As seguintes opções permitem editar e visualizar o texto em HTML:

- **Editar HTML com Êxito**—Abre o Editor HTML que você pode usar para formatar o HTML.
- **Exibição rápida**—Visualiza o HTML.
- **Código-fonte HTML**—Mostra o código-fonte HTML.

Texto com falha

Especifica o conteúdo de texto sem formatação de uma mensagem de resposta quando a mensagem não for processada com êxito.

HTML com falha

Especifica o conteúdo HTML de uma mensagem de resposta quando a mensagem não for processada com êxito. As seguintes opções permitem editar e visualizar o texto em HTML:

- **Editar HTML com falha**—Abre o Editor HTML que você pode usar para formatar o HTML.
- **Exibição rápida**—Visualiza o HTML.
- **Código-fonte HTML**—Mostra o código-fonte HTML.

Observação: para mais informações sobre as regras de validação da caixa de correio, consulte o *Guia de Administração*.

5. (Opcional) Crie ou atualize as regras e as políticas da caixa de correio conforme o adequado.

   Observação: ao criar as regras da caixa de correio, você as associa a uma caixa de correio específica—outra caixa de correio não pode compartilhar essas regras. Se desejar usar regras que pertencem a uma caixa de correio para uma caixa de correio diferente, recrie-as para a outra caixa de correio.

   Importante: Recomendamos que você configure a respectiva caixa de correio como Inativa antes de configurar uma regra de caixa de correio. Caso contrário, quaisquer mensagens que o servidor de email recuperar entre sua primeira mudança e a última mudança serão processadas com quaisquer regras que estiverem em vigor quando a mensagem for recuperada.

6. Clique em Salvar.

   As mudanças à caixa de correio padrão são salvas e aplicadas. A primeira consulta ocorre após um segundo.

Várias caixas de correio

CA SDM pode processar e gerenciar diversas caixas de correio. Cada caixa de correio possui sua própria definição, em vez de usar um único conjunto global de definições. É possível definir diversas caixas de correio e usar diferentes modelos ou valores padrão para cada caixa de correio. Diversas definições permitem a inquilinos individuais usar caixas de correio separadas, ou permitem que um inquilino ou organização usem diferentes caixas de correio e possuam diferentes comportamentos para cada caixa de correio. É possível configurar diversas caixas de correio usando a interface Administração. Cada caixa de correio usa as seguintes tabelas:

- usp_mailbox — define a caixa de correio.
- usp_mailbox_rule — especifica um conjunto de regras para cada caixa de correio.

  Porque as regras da caixa de correio fornecem padrões de API de texto, é possível estabelecer interfaces de email com outros softwares e parâmetros (como categoria, responsável, e assim por diante) que são configurados especificamente para a interface.

Observação: os servidores IMAP oferecem suporte a diversas caixas de correio para uma única conta, mas caixas de correio alternativas não são suportadas; apenas a caixa de entrada padrão é suportada.

Como várias caixas de correio usam regras

O componente do Mail Eater (pdm_maileater_nxd) no servidor principal usa conexões e regras da caixa de correio para ler e processar mensagens de uma ou mais contas em um ou mais servidores de correio. O Mail Eater processa caixas de correio em série (apenas uma caixa de correio é processada por vez), e processa regras em uma ordem de número em sequência.

Diversas caixas de correio usam regras como segue:

1. À inicialização do servidor principal, o Mail Eater lê as seguintes tabelas:

   usp_mailbox

   Representa uma conexão ao servidor de correio.

   usp_mailbox_rules

   Representa as regras que se aplicam à conexão (usp_mailbox).

   Contact_Method

   Representa os Métodos de contato usados para respostas automáticas.

   Document_Repository

   Representa os Repositórios de documento para armazenar anexos.

   O Mail Eater detecta automaticamente mudanças a objetos em quaisquer dessas tabelas, incluindo a adição de objetos adicionais. Se for realizada uma mudança a usp_mailbox ou usp_mailbox_rule, o intervalo de pesquisa para a caixa de correio afetada é reprogramado para um segundo após a mudança ser aplicada.

2. Ao intervalo definido por cada caixa de correio, o Mail Eater recupera cada email na caixa de entrada para conta associada e processa o email como segue:

   a. Verifica o endereço de email quanto a violações de política. Quando o Mail Eater encontra uma violação, o processamento para e um log padrão é afetado de acordo com a definição da caixa de correio.

   b. Compara o email a cada regra (mailbox_rule) que pertence àquela caixa de correio.

   c. Se uma regra correspondente for encontrada, envia a mensagem à API de texto para postagem e responde ao usuário, conforme for adequado, com base na ação especificada para a regra.

      Para responder emails, a sequência de caracteres de filtro identifica o objeto e usa a API de texto para processamento. Após o processamento estar concluído, a resposta vai para os endereços de Responder a De.

   d. Após o Mail Eater encontrar uma regra correspondente, nenhuma outra regra é verificada, e o Mail Eater processa o próximo email na caixa de entrada.

   e. Se nenhuma regra correspondente for encontrada, a mensagem é descartada.

3. Após o Mail Eater processar todos os emails para uma caixa de entrada, as mensagens processadas e descartadas são eliminadas e o próximo intervalo de processamento é programado.

Como configurar respostas de emails

As notificações de email que você usa em caixas de correio são específicas para respostas enviadas para um contato em resposta aos emails dele. Você pode configurar email de modo que, quando um contato clica em um link de resposta em uma notificação de email, o email de resposta é direcionado a uma caixa de correio.

Observação: essa configuração difere das notificações de email regulares.

Você usa Administração do CA SDM para configurar o email como segue:

1. Crie uma caixa de correio para processar email recebido em um servidor.
2. Navegue para Gerenciador de opções, Email e configure o servidor de correio de envio.
3. (Opcional) Especifique um endereço de email de notificação na definição de contato.
4. Navegue para Notificações, Métodos de notificação, Email e crie ou atualize um método de notificação que inclua as seguintes configurações:
   - Oferece suporte a SMTP—ativado
   - pdm_mail [–F *from_email_address*] [–T *reply_to_email_address*]

     from_email_address

     Especifica o endereço usado como o endereço De da mensagem. Esse endereço substitui o endereço do remetente na configuração de servidor de correio de envio.

     reply_to_email_address

     Especifica o endereço para o qual as respostas são enviadas. Esse endereço substitui o endereço responder para na configuração de servidor de correio de envio.

     Quando um endereço responder para é definido na configuração do servidor de correio de envio e nenhum endereço responder para é especificado no Método de notificação, o endereço responder para na configuração do servidor de correio de envio é usado com esse Método de notificação.

- Palavra-chave “$(REPLY_FROM)”

  Se a palavra-chave “$(REPLY_FROM)” for especificada como qualquer dos endereços, esse endereço é criado a partir do nome de usuário e do nome de host do servidor de correio para a caixa de correio. Essa palavra-chave somente é válida quando uma regra da caixa de correio usa o Método de notificação; Métodos de notificação que a usam não devem ser usados para qualquer outro fim. Por exemplo, user name=dev, server name=mail32.ca.com, $(REPLY_FROM)=dev@mail32.ca.com. Somente use essa palavra-chave se seu servidor de correio estiver configurado para aceitar o nome de servidor de correio como equivalente ao nome de domínio de email. Use essa palavra-chave com cuidado: se o nome do host não for totalmente estendido para domínio na configuração da caixa de correio (por exemplo, mailserver1, em vez de mailserver1.customer7.com), ele não é estendido automaticamente pelo interpretador do campo.

Observação: o from_email_address e o reply_to_email_address são os endereços que aparecem nos cabeçalhos De e Responder para da mensagem quando o usuário a lê. Se os endereços forem idênticos, você pode especificar somente o from_address.

5. Navegue para Email, Regras da caixa de correio, abra cada regra da caixa de correio aplicável e selecione o novo método de resposta na lista suspensa Resposta. Salve cada regra de atualização.

   Quando o contato responde à notificação de email, a resposta é endereçada por padrão à caixa de correio especificada.

Mais informações:

Utilitário pdm_mail - Enviar notificação de email (na página 107)

Identificação de endereço de remetente alternativo

É possível usar um parâmetro -m no assunto da mensagem para que o CA SDM identifique o remetente da mensagem usando um endereço de email diferente daquele usado originalmente para enviá-la. A palavra-chave -m, seguida por um espaço e o endereço de email que o CA SDM reconheça, devem ser os últimos elementos da linha de assunto. Considere as seguintes informações ao usar o parâmetro -m no assunto:

- Tanto o endereço De como o endereço alternativo com -m são verificados nas listas de Inclusão e Exclusão.
- O endereço de email especificado como o endereço alternativo deve conter somente o endereço, e não o nome de exibição que o acompanha.
- Se mais de uma palavra seguir-se ao parâmetro -m na linha de assunto, o endereço alternativo não é reconhecido.

Objetos

Um *objeto* de email refere-se a algo que surge do processo de correio, por exemplo, um endereço de email que é incluso em um email encaminhado. A API de texto usa objetos que contêm uma ID de ticket (como número de referência) para suporte a resposta. Quando a ID de ticket é encontrada, uma palavra-chave da API de texto existente (como %INCIDENT_ID) é definida e adicionada à entrada para a API de texto. O Mail Eater identifica que uma resposta está associada a um ticket em particular encontrando o objeto na mensagem.

As regras da caixa de correio permitem especificar o objeto e o valor que a API de texto usa. Por exemplo, você pode definir uma regra para incidentes como Incident:{{object_id}}%. Quando uma regra encontra Incident:1234, a API de texto usa %INCIDENT_ID=1234 (1234 é o ref_num para o Incidente). Porque o objeto deve ser único em um email e fácil de encontrar, você pode tornar o objeto mais distinto, como %Incident:{{object_id}}%. Um sinal de percentagem (%), espaço em branco ou algum outro caractere que não apareça e um valor de objeto deve se seguir {{object_id}}. Letras maiúsculas e minúsculas, números, barras, vírgulas e sinais de mais são potencialmente parte de um valor. Os objetos seguros são codificados em Base64 após a criptografia. Se você não usa objetos Seguros, os caracteres que seguem o objeto não devem estar contidos no sufixo na ID do ticket, se houver, que foi configurado para esse tipo de ticket.

Ao usar a sequência de caracteres de filtro das regras da caixa de correio para identificar o Objeto da ID do ticket, a palavra-chave {{object_id}} representa a posição no sequência de caracteres do filtro onde o objeto da ID do ticket é esperado. Essa palavra-chave diferencia entre maiúsculas e minúsculas, mesmo se a regra da caixa de correio não diferenciar.

Exemplo: uso do objeto de email

O exemplo a seguir mostra um formato ARTIFACT para uso em uma regra de caixa de correio para um ticket de solicitação de mudança.

Uso: %REQUEST=@{call_req_id.ref_num}%

Exemplo: %REQUEST=1234%

Considerações sobre uso de objetos

Ao criar a sequência de caracteres do filtro na regra de caixa de correio, considere o seguinte:

- Um limite claro deverá existir entre o objeto da ID do ticket e as palavras-chave que o envolvem. Recomendamos incluir texto com espaços em branco neste texto de limite.
- Não termine a porção da sequência de caracteres do filtro que precede a palavra-chave {{object_id}} em um padrão opcional ou que possa ser repetido que possa corresponder ao início do objeto da ID do ticket, e não termine um padrão cujo comprimento for ambíguo. Por exemplo, a sequência de caracteres do filtro não pode conter request(er|ed|ing)?{{object_id}} porque esta construção causa uma ambiguidade em relação a se er, ed ou ing à esquerda é o final do texto ou parte do prefixo de uma ID de ticket não protegida.

- A porção da sequência de caracteres do filtro que se segue à palavra-chave {{object_id}} não pode iniciar em um padrão opcional ou que possa ser repetido, e que possa corresponder ao final do objeto ID do ticket, não deve começar com um padrão cujo comprimento seja ambíguo e deve conter pelo menos um elemento de espaço em branco. Por exemplo:
  - A sequência de caracteres do filtro não pode conter {{object_id}}[A-Z]?, porque [A-Z]? pode corresponder ao último caractere do objeto ID do ticket.
  - A sequência de caracteres do filtro não pode terminar com {{object_id}}Item, porque é possível que Item apareça no objeto ID do ticket, seja como sufixo de um objeto ID de ticket em texto sem formatação ou protegido, seja como caracteres dentro de um objeto seguro.
  - {{object_id}} Item é aceitável, porque o espaço não pode ser parte de um objeto ID de ticket, e não é parte de um objeto ID de ticket protegido ou em claro. No entanto, {{object_id}}[\t\r\n]+Item (colchete, espaço, barra invertida, t, barra invertida, r, barra invertida, n, colchete, sinal de mais, +Item) é melhor, porque o [\t\r\n]+ compensa a inserção de uma quebra de linha pelo programa de correio depois de {{object_id}}.
- Ao criar sequências de caracteres de filtro para diferentes regras de caixa de correio, evite usar uma sequência de caracteres de filtro que inclua completamente outra sequência de caracteres de filtro para diferentes regras de caixa de correio, ou na qual a porção antes ou depois de uma palavra-chave {{object_id}} inclua completamente aquela porção de outra sequência de caracteres de filtro de regra de caixa de correio. Dependendo da ordem na qual estes filtros são verificados, uma mensagem destinada a um filtro pode coincidir com outro filtro, com uma porção do objeto ID do ticket que coincida com o texto adicional que distingue entre duas sequências de caracteres de filtro.

Proteção e segurança de artefatos

Você usa artefatos para proteger a entrega de correio a uma caixa de correio das seguintes maneiras:

- Use a palavra-chave ARTIFACT em notificações e frases de notificação.

  Observação: o nível de segurança do artefato deve corresponder à configuração Tipo de artefato mínimo das regras da caixa de correio para a caixa de correio para a qual os emails são enviados. Tipos mais seguros que o definido são permitidos. Em outras palavras, se você definir ARTIFACT=PROTECTED, então tanto PROTECTED quanto SECURE são permitidos, mas NONE não é permitido.

- Defina a opção Tipo de artefato mínimo em Detalhes das regras das caixas de correio.

É possível integrar um artefato em uma frase de notificação e especificar o nível de segurança para o artefato, por exemplo:

%REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%

Observação: para obter mais informações sobre as tabelas para a opção Tipo de artefato mínimo (filter_min_artifact_type) e Detalhes das regras das caixas de correio (usp_mailbox_rule table), consulte o *Guia de Referência Técnica*.

Exemplo: nenhuma validação de artefatos

O exemplo a seguir não mostra nenhum formato ARTIFACT. Nenhuma validação de artefatos pode ser realizada.

Uso: %REQUEST=@{call_req_id.ref_num}%

Exemplo: %REQUEST=1234%

Exemplo: nenhuma validação de artefatos

O exemplo a seguir apresenta o formato ARTIFACT=NONE. ARTIFACT=NONE é o mesmo que não adicionar a palavra-chave; nenhuma validação de artefatos pode ser realizada.

Uso: %REQUEST=@{ARTIFACT=NONE:call_req_id.ref_num}%

Exemplo: %REQUEST=1234%

Exemplo: validar um número de ticket com relação ao hash para confirmação

O exemplo a seguir apresenta o formato ARTIFACT=PROTECTED. O formato PROTECTED valida um ticket com relação ao hash para confirmação. A letra "A" denota o tipo de formatação. Vírgulas separam "A", o código do hash, e o número do ticket.

Uso: %REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%

Exemplo: %REQUEST=A,12345678,1234%

Exemplo: criptografar o número de ticket

O exemplo a seguir apresenta o formato ARTIFACT=SECURE. O formato SECURE criptografa o ref_num, e então codifica o resultado em uma codificação Base64, de modo que possa ser incluído com segurança no texto da mensagem. A letra "B" denota o tipo de formatação. Vírgulas separam "B" e um número de ticket criptografado por senha.

Uso: %REQUEST=@{ARTIFACT=SECURE:call_req_id.ref_num}%

Exemplo:
%REQUEST=B,da1jhr+9U5GVfd2VGH4dsnx2+PaSvygDS2e3IqjpjtyNSDW2u/KNPX61nopDu/KB%

Contratos de nível de serviço

Um SLA (service level agreement - contrato de nível de serviço) ou tipo de serviço é um acordo entre uma central de serviços e seus clientes, e normalmente descreve o nível de serviço a ser fornecido pela central de serviços. Se esse nível de serviço não for fornecido, o service desk poderá ser penalizado. Por exemplo, um service desk que fatura de acordo com “pagamento por serviço realizado” pode não receber o pagamento total por um serviço que não atenda ao nível estabelecido no contrato de nível de serviço. Sendo assim, a maioria dos service desks leva muito a sério os contratos de nível de serviço e se esforça para fornecer o tipo de serviço especificado nesses contratos.

Além disso, a maioria das centrais de atendimento mantém um registro meticuloso do cumprimento ou violação de contratos de nível de serviço. Os tipos de serviço definidos com o CA SDM são projetados para ajudar a equipe do service desk a cumprir seus contratos de nível de serviço e manter os registros de que necessitam para verificar se os contratos de nível de serviço estão sendo cumpridos.

Utilização do SLA

No CA SDM, você define SLAs usando tipos de serviço e eventos para fazer o seguinte:

- Use eventos para monitorar tickets.
- Use tipos de serviço para acompanhar compromissos e programações de fornecedores e empresas, pois eles se relacionam com tickets específicos.
- Estabelecer controles de data e hora para processar eventos e tipos de serviço.

O CA SDM permite que você projete e use SLAs como segue:

- **Contratos de nível de serviço para várias organizações**—É possível atribuir diferentes Tipos de serviços para cada campo de referência dependendo da organização afetada do ticket. Por exemplo, o Tipo de serviço de um ticket com Prioridade 1 pode ser diferente para a Organização A e Organização B.
- **Acompanhamento de vários SLAs**—Um ticket pode acompanhar vários Tipos de serviço de uma vez, assegurando que todos os aspectos de um SLA negociado sejam visíveis.
- **Projeções de Tempo até violação**—Um subsistema que monitora tickets constantemente no CA SDM, e registra quando seus SLAs entram em violação com base em seu estado atual.
- **Custo de violação do SLA**—Este campo de Tipo de serviço ajuda com métricas e na determinação da gravidade de tickets abertos.
- **Tipos de serviço em tarefas**: os Tipos de serviço estão disponíveis em tarefas de fluxo de trabalho (na página 296).
- **Alvos de serviço—**Tipos de serviço também podem ter um ou mais Alvos de serviço para medir se o serviço ou conserto solicitado foi completado dentro do prazo de tempo necessário.

Processamento do SLA clássico

No processamento "clássico" de SLA (ativado se a opção classic_sla_processing estiver instalada no Gerenciador de opções) somente um tipo de serviço pode ser aplicado a um ticket em um dado momento. Quando atributos diferentes de um ticket têm tipos de serviço diferentes a eles associados, o tipo de serviço com a classificação mais alta será utilizado. A classificação de um tipo de serviço é definida quando o tipo de serviço é criado, com a classificação mais alta sendo 1, a seguinte 2 e assim por diante. Por exemplo, suponha que uma ocorrência que possui um tipo de serviço de resolução em 12 horas (classificação 2), tenha sido atribuída a uma prioridade de código 1, que possui um tipo de serviço de resolução em 4 horas (classificação 1). O tipo de serviço com a classificação mais alta determinará o comportamento do serviço para a ocorrência associada. Nesse exemplo, a resolução em 4 horas tem uma classificação mais alta do que a resolução em 12- horas, portanto, o tipo de serviço de resolução em 4 horas será aplicado à ocorrência.

Observação: para obter mais informações sobre a opção *classic_sla_processing*, consulte a Ajuda online.

Tipos de serviço e eventos

Para controlar agendamentos e compromissos de fornecedores e da organização relacionados a tickets específicos, você pode anexar eventos a tipos de serviço. Os tipos de serviço fornecem uma forma eficiente e flexível de anexar automaticamente os eventos ao ticket.

Os tipos de serviço oferecem suporte automatizado aos contratos de nível de serviço que você estabeleceu com seus clientes. Ao usar tipos de serviço, você pode monitorar qualquer aspecto de uma situação relacionada a um período de tempo ou- a uma condição. Por exemplo, você pode definir uma política que defina um tempo de resolução para uma dada ocorrência e associar a ela uma ação. Os tipos de serviço fornecem a capacidade de administrar fornecedores de serviço, fornecedores de produtos e o próprio service desk, proporcionando modos de avaliar o desempenho e o nível de adoção das diretivas.

Tipos de serviço permitem:

- Identificar automaticamente o nível de serviço necessário a tickets específicos
- Identificar condições de violação do nível de serviço

- Enviar automaticamente notificações de aviso antes da expiração de contratos de nível de serviço
- Configurar relatórios de violação de contrato de nível de serviço

Como implementar tipos de serviço

Os tipos de serviço permitem definir ações com base em condições definidas pelo usuário. Os tipos de serviço podem ser aplicados aos tickets. Por exemplo, você pode definir um tipo de serviço que especifique o tempo de resolução de um dado ticket e, em seguida, associar um comportamento que ocorra automaticamente quando a ação ocorrer, como uma notificação a uma pessoa de apoio sobre uma violação pendente. Como os tipos de serviço podem englobar diversos eventos, e os eventos podem conter várias ações (se verdadeiro ou falso), é possível definir comportamento mais complexo adicionando vários eventos a tipos de serviço.

Para implementar tipos de serviço, faça o seguinte:

1. Associe um tipo de serviço ao respectivo atributo. Vários tipos de serviço podem ser definidos e classificados em relação uns aos outros.
2. Atribua os tipos de serviço a ICs, contatos, organizações, categorias de ocorrência, categorias de mudança, áreas de solicitação e prioridades. Cada registro pode ser atribuído a um único tipo de serviço.
3. Definir condições específicas que determinem quando um contrato de nível de serviço é cumprido ou violado.
4. Identificar ações que devem ser realizadas para ajudar o service desk a cumprir seus contratos de nível de serviço.
5. Realizar as ações adequadas para impor os contratos de nível de serviço automaticamente.

Exemplo: associe um tipo de serviço a um contato

Neste exemplo, você realiza as seguintes etapas para associar um tipo de serviço a um contato:

1. Atribua um tipo de serviço na página Detalhes do contato.

   Quando o contato for atribuído a um ticket, o campo Tipo de serviço será automaticamente preenchido com o tipo de serviço atribuído no registro do contato.

2. Insira Alfa, Beta como o nome no campo Usuário final afetado na página Detalhes da ocorrência e salve a ocorrência.

   O campo Tipo de serviço é preenchido automaticamente com o valor definido neste registro de contato. Você pode substituir o valor padrão selecionando outros tipos de serviço.

Tipos de serviço predefinidos

O CA SDM fornece tipos de serviço predefinidos. É possível modificar os tipos de serviço predefinidos e criar tipos de serviço que melhor sejam mais adequados às necessidades de sua empresa. Os seguintes tipos de serviço predefinidos estão incluídos com o CA SDM:

- Resolução em 4 horas
- Resolução em 12 horas
- Resolução em 48 horas
- Resolução em 72 horas

O tipo de serviço Resolução em 4 horas está associado ao código de prioridade 1 logo após a instalação do CA SDM, o que significa que os tickets criados com uma prioridade 1 são tratados como se devessem ser resolvidos em quatro horas. Vários eventos de tipo de serviço estão associados ao tipo de serviço Resolução em 4 horas para garantir uma resolução rápida:

- A pessoa para a qual o ticket foi criado será notificada de que pode esperar uma resolução em até quatro horas.
- O gerente do grupo será notificado caso o ticket não seja atribuído em até 30 minutos.

- Uma notificação de aviso será enviada ao destinatário e ao gerente do grupo caso o ticket não seja resolvido em 3,5 horas.
- Finalmente, uma notificação de violação será enviada ao destinatário e ao gerente do grupo se o ticket não tiver sido resolvido em 4 horas, e o sinalizador Violação do contrato associado ao ticket será ativado.

Nenhum dos outros tipos de serviço predefinidos estão associados a um código de prioridade, porém eles são definidos com eventos semelhante aos descritos para o tipo de serviço Resolução em 4 horas. Como um administrador de sistema, você poderá associar esses tipos de serviço a códigos de prioridade se desejar. Por exemplo, você poderá fazer as seguintes associações:

- Prioridade 2 - resolução em 2 a 12 horas
- Prioridade 3 - resolução em 3 a 48 horas
- Prioridade 4 - resolução em 4 a 72 horas

Por outro lado, você pode remover a associação entre o código de prioridade 1 e o tipo de serviço de resolução em 4 horas, caso não atenda às suas necessidades.

As opções de personalização cr_sla, chg_sla e iss_sla especificam que todas as solicitações, requisições de mudança e ocorrências sejam associadas a um tipo de serviço. Essas opções selecionam o melhor tipo de serviço e o associam à solicitação, requisição de mudança ou ocorrência. Essas opções são instaladas automaticamente, no entanto, você pode desinstalá-las ou reinstalá-las usando o Gerenciador de opções.

Observação: para obter descrições sobre as opções de personalização, consulte a *Online Help*. Para obter informações sobre como definir tipos de serviço e modificar códigos de prioridade, consulte a *Ajuda online*.

Configuração de eventos

O CA SDM usa condições e ações definidas como eventos para agendar, processar e rastrear tickets e tipos de serviço automaticamente. Cada evento tem três características de comportamento genéricas: condições, ações quando verdadeiro e ações quando falso. Além disso, um tempo de espera é associado à condição (e portanto, ao evento) e medido a partir do momento em que o ticket é salvo. O tempo de espera determina quando a condição é avaliada. Você também pode criar eventos automáticos para que uma ação específica ocorra sempre que um evento específico ocorrer. Por exemplo, você pode fazer com que uma notificação ocorra automaticamente para uma ocorrência transferida com uma prioridade P1 que permaneça aberta por mais de uma hora.

- As *condições* identificam o evento para qual o CA SDM deve estar preparado.

  Uma condição é qualquer estado mensurável de um ticket. Um ticket com um estado “não atribuído” é um exemplo de uma condição. Essa condição pode ser associada a uma ação que ocorra quando a condição for verdadeira ou quando ela for falsa. Por exemplo, no tipo de serviço predefinido Resolução em 12 horas, há um evento associado chamado "não atribuído 1 hora" com “Ocorrência não atribuída” como sua condição. A ação definida para esse evento é notificar o gerente do grupo responsável pela ocorrência se a condição for verdadeira, com um tempo de espera de uma hora. Se a Resolução em 12 horas fosse atribuída a uma ocorrência, o comportamento seria “despertar” uma hora após o registro ter sido salvo, verificar se ele ainda não estava atribuído e notificar o gerente do grupo caso essa ocorrência ainda não tenha sido atribuída.

- As *ações* identificam os processos que ocorrem automaticamente quando a condição é verdadeira ou falsa após um determinado período de tempo.

  Você pode atribuir uma única ação ou uma lista de ações a serem realizadas para cada evento controlado. Quando um evento que corresponda à condição ocorre, o CA SDM processa automaticamente as ações associadas à condição. Em alguns casos, as ações automaticamente processam o objeto ou fazem com que notificações sejam criadas.

Alguns dos eventos predefinidos para ocorrências são mostrados na tabela a seguir. Há eventos predefinidos similares para solicitações e requisições de mudança, e vários outros eventos relacionados aos tipos de serviço predefinidos:

Event	Descrição
P1 ativo - Notif destin ocorr	Notifica o destinatário de que a ocorrência já está ativa há mais de 1 hora e tem uma prioridade 1.
P2 ativo - Notif destin ocorr	Notifica o destinatário de que a ocorrência já está ativa há mais de 1 dia e tem uma prioridade 2.
Não atrib.- Transf. de ocorr.	Transfere ocorrências que permaneçam não atribuídas por mais de 1 dia; notifica o destinatário, o criador da ocorrência e o novo destinatário.

Uma vez definidos, esses eventos podem ser anexados manual ou automaticamente a tickets e tipos de serviço, como acontece com tipos de serviço predefinidos. Vários eventos podem ser anexados a cada tipo de serviço.

Importante: Não use o Gerenciador de opções para instalar eventos automáticos até que os eventos sejam criados. Ativar eventos automáticos antes que existam prejudica seriamente o desempenho. Para obter mais informações sobre como definir eventos, e opções de evento como auto_events, chg_auto_events e iss_auto_events, consulte a *Ajuda online*.

Mais informações:

Uso do Gerenciador de opções (na página 381)

Como criar Metas de serviço

Para minimizar violações de SLA, você pode criar um conjunto de modelos de destino de serviço para medir cada estágio de resolução de ticket. Como os Tipos de serviço, cada meta de serviço contém uma condição e estimativa do tempo para conclusão. No entanto, as metas de serviço não fornecem um mecanismo de ação.

Durante a criação de ticket, um Tipo de serviço atribui uma ou mais metas de serviço para acompanhar cada estágio da resolução do ticket. Cada vez que o ticket muda, as metas de serviço ativas avaliam a condição. Se a condição for atendida, o ticket e o log de atividade mostram o horário de conclusão real. Quando o tempo excede o horário estimado, o ticket mostra a quantidade de tempo pela qual a meta não foi alcançada.

As metas de serviço permitem fazer o seguinte:

- Verificar se os tickets do mesmo Tipo de serviço seguem as mesmas metas de serviço.
- Monitorar se os tickets são fechados dentro dos intervalos de tempo obrigatórios.
- Exibir informações tais como o número de minutos restantes antes da conclusão de uma meta de serviço.

Ao criar modelos de meta de serviço, considere:

- Considere o resultado necessário para atingir a meta de serviço. Use uma Condição ou uma Macro de condição definida pelo local existentes para avaliar os dados do ticket. Se necessário, personalize ou grave uma nova macro para gerenciar a meta de serviço.
- Calcule os custos projetados de violação e multa com base nos contratos de SLA.
- Atribua pelo menos um modelo de meta de serviço a um Tipo de serviço.

Para criar um modelo de meta de serviço, faça o seguinte:

1. Crie um modelo de meta de serviço para gerenciar solicitações, incidentes, problemas, requisições de mudança ou ocorrências.
2. Vincule o modelo de meta de serviço a um Tipo de serviço.
3. Atribua o detalhe de um modelo de meta de serviço a uma categoria de ticket como tickets de solicitação, incidente, problema, requisição de mudança ou ocorrência.

   No momento da criação do ticket, o modelo adequado é anexado automaticamente ao ticket com base no Tipo de serviço. Sempre que um usuário cria um ticket, o status da meta de serviço é exibido automaticamente na guia Tipo de serviço.

Contratos de serviço

O modelo de SLA inclui o Contrato de serviço. O Contrato de serviço define o SLA para uma determinada organização e inclui seus tipos de serviço, áreas de solicitação e categorias de ocorrência ou mudança. Essas definições são denominadas Categorias *privadas* e Tipos de serviço *privados*.

Observação: as Categorias e os Tipos de serviço *privados* só podem ser usados em tickets para os quais o Contrato de serviço está em vigor.

O Contrato de serviço associado a um ticket é determinado pela *organização afetada* pelo ticket, a qual é sempre a organização do Usuário final afetado pelo ticket (isso é representado pelo campo Organização em um registro de Contato). Apenas as áreas ou categorias listadas no Contrato de serviço podem ser selecionadas para o ticket. Além disso, os únicos Tipos de serviço que podem ser aplicados são os *privados* listados no Contrato. Isso assegura que os SLAs de uma organização não sejam acidentalmente confundidos com os de outra empresa.

Um Contrato de serviço também associa Tipos de serviço a campos de referência comuns em um ticket, como Prioridade e Ativo. Este mapeamento associa Tipos de serviço com atributos de um ticket. Por exemplo, o contrato de uma organização pode atribuir Tipos de serviço a cada um dos cinco objetos de Prioridade. Quando um ticket é criado com uma determinada prioridade, o Tipo de serviço associado é selecionado.

Categorias e Tipos de serviço podem ser definidos fora de um contrato, quando são como *públicos.* As definições públicas são usadas quando um ticket não tem um Contrato de serviço. A falta de um Contrato de serviço pode ocorrer se o usuário final não tem uma organização, ou se o contrato da organização estiver inativo. Uma definição pública é um backup útil ou um mecanismo padrão. Os Tipos de serviços públicos são definidos diretamente em categorias e outros objetos de campo de referência.

Todos os tipos de serviço aplicáveis são atribuídos ao ticket. Isso garante que todos os aspectos de um SLA estejam visíveis e sejam aplicados, por exemplo:

- Uma Impressora pode ter um Tipo de serviço que exige uma visita do técnico a ser feita em até 2 dias.
- O Tipo de serviço de um objeto de prioridade pode exigir um retorno de chamado em até 1 hora.

Ao aplicar ambos esses Tipos de serviço, é possível garantir que essas ações necessárias sejam realizadas.

O rastreamento de múltiplos Tipos de serviço também ajuda a dar prioridade aos tickets. Por exemplo, um Tipo de serviço de baixa prioridade é atribuído a um ticket associado a um teclado quebrado. No entanto, se o usuário final afetado precisar de um teclado com urgência, a prioridade do serviço pode ser aumentada.

Observação: o modelo de SLA é aplicado por padrão. Versões passadas do CA SDM associavam apenas um único Tipo de serviço a um ticket. A seleção de Tipo de serviço envolvia localizar o Tipo com a mais alta *classificação* entre todos os Tipos de serviço existentes. Um modelo usando um esquema de classificação ainda pode ser usado instalando a opção ‘classic_sla_processing’.

Migração de contratos de serviço

Se o CA SDM foi instalado como parte de uma migração, a opção classic_sla_processing estará ativada por padrão, portanto, seu processamento de SLA será como sempre era antes da migração.. Isso lhe dará tempo de criar contratos de serviço apropriados e, eventualmente, desativar a opção classic_sla_processing.

Ao criar contratos de serviço, você não terá de criar novos tipos de serviço, áreas de solicitação ou categorias. Você poderá usar o botão Copiar nos detalhes do Contrato de serviço para copiar objetos existentes no contrato.

Se a instalação anterior marcou o campo support_lev como necessário para todos os tipos de tickets, essa restrição deverá ser removida. O campo support_lev ainda existe, porém não está definido no modelo atual, portanto, um erro de campo obrigatório ocorrerá em novos tickets. Isso afeta os objetos Solicitação, Ocorrência e Requisição de mudança.

Horário para violação

Quando o modelo de SLA está em uso, o sistema de Tempo para violação (TTV) do CA SDM pode ajudá-lo a acompanhar e dar prioridade a tickets de acordo com seu tempo para violação previsto. Esse sistema monitora todos os tickets ativos e define o tempo para violação previsto para cada Tipo de serviço. Você pode registrar e classificar tickets de acordo com seu tempo para violação e custo, o que ajuda a dar prioridade à resolução de ocorrências urgentes e de alto custo.

O sistema TTV monitora todos os tickets ativos e avalia de modo silencioso seus eventos de SLA, determinando que eventos apresentarão o sinalizador Violação do contrato de nível de serviço. Isso não faz com que os eventos sejam executados, o sistema apenas avalia o resultado de cada evento com base no estado atual do ticket. Se a avaliação resultar em uma ação que ative o sinalizador Violação do SLA, o Tipo de serviço anexado ao ticket é atualizado com um valor de Tempo para violação. Esse valor é a data/hora quando a violação do contrato será ativada.

A avaliação ocorre sempre que um ticket é inserido ou atualizado. Como os tickets são atualizados com frequência em rápida sucessão, a avaliação é suspensa por um curto período. O intervalo de suspensão (atraso) é controlado pela opção ttv_evaluation_delay. Após o período de suspensão, o sistema TTV avalia todos os eventos de Contrato de nível de serviço que possam ativar o sinalizador Violação do contrato.

Cada evento tem uma condição opcional e um conjunto de ações (Macros) que são ativadas de acordo com o resultado da condição. Para garantir um desempenho adequado, as informações de modelo do evento são colocadas no cache pelo sistema TTV e são atualizadas periodicamente. As previsões feitas pelo TTV quanto a modelos de evento recentemente atualizados podem estar incorretas durante vários minutos.

Observação: as projeções do TTV aparecem na guia Tipo de serviço de cada ticket. O sistema TTV é ativado pela opção ttv_enabled.

Fusos horários e turnos de trabalho

Para atender às complexas exigências de negócios quanto à execução automatizada de aplicativos, o CA SDM permite definir vários fusos horários e turnos de trabalho conforme necessário, além de registrá-lo como fácil referência.

- Os fusos horários identificam o fuso horário onde o usuário, IC, etc. estão localizados.
- Os turnos de trabalho definem o período durante o qual a monitoração de evento é feita ou o horário de trabalho associado a um tipo de serviço ou contrato de nível de serviço.

Ser capaz de determinar que ação executar de acordo com o momento em que um evento ocorre pode ser fundamental no tratamento adequado do evento. Os fusos horários e turnos de trabalho que você definir estarão disponíveis para uso por qualquer uma das funções do CA SDM.

Mais informações:

Fusos horários (na página 368)
Configurar turnos de trabalho (na página 185)

Configuração de fusos horários

Os códigos de fuso horário definem o fuso horário no qual um usuário normalmente acessa o sistema (isto é, o fuso horário local do usuário) ou o fuso horário em que um IC está localizado. Os horário comerciais são sempre inseridos de acordo com o fuso horário do servidor do CA SDM. Isso significa que o horário comercial sempre poderá ser comparado de modo uniforme.

Os fusos horários são usados para administrar tipos de serviço, escalonamentos e a resposta geral a usuários finais afetados com base na capacidade do CA SDM de apresentar a hora correta em vários fusos horários. O CA SDM ajusta automaticamente a diferença entre o fuso horário onde um usuário faz o logon ou um IC está localizado e o fuso horário do local onde o servidor está sendo executado. Os fusos horários usam o formato Tempo Médio do Meridiano de Greenwich (GMT).

Observação: para obter informações sobre como definir fusos horários, consulte a *Ajuda online*.

Como gerenciar diversos fusos-horários para tipos de serviço

Os servidores e os usuários do CA SDM podem estar localizados em diferentes fusos-horários. A diferença de hora pode fazer os usuários perderem datas e horas de expiração do Tipo de serviço.

Para corrigir a diferença de hora, é possível configurar o CA SDM para exibir horas de expiração de Tipo de serviço no fuso-horário do usuário final. Se dois usuários em fusos-horários diferentes virem o mesmo ticket, cada usuário verá os valores de Hora de expiração com base no fuso-horário do computador local. Entretanto, os valores de Hora de início sempre refletem o fuso-horário do servidor.

Para configurar para o fuso-horário do usuário final, faça o seguinte:

1. Crie um código de servidor que identifique o nome do servidor e o fuso-horário.
2. Crie ou atualize o Tipo de serviço. Defina o campo Usar fuso horário de usuário final como Sim.

   Um valor de Sim faz Hora de expiração exibir e atualizar de acordo com o fuso-horário de cada usuário final.

Exemplo: mostrar datas de expiração de Tipo de serviço no fuso-horário de qualquer usuário

Neste exemplo, você configura o CA SDM para mostrar datas de expiração de Tipo de serviço no fuso-horário de qualquer usuário. O servidor e o usuário estão em computadores separados e em diferentes fusos-horários.

Para criar um código de servidor que identifique o nome do servidor e o fuso-horário.

1. Na guia Administração do servidor de host, selecione Service Desk, Código do aplicativo.
2. Clique em Códigos, Servidores.

   A Lista de servidores é exibida.
3. Clique no servidor do Host local.

   A página Detalhes do nome do servidor aparece.
4. Especificar o fuso-horário. Por exemplo, definir o fuso-horário para GMT (EU). O nome de host local deve corresponder ao valor NX_LOCAL_HOST armazenado no NX.env para o servidor
5. Clique em Salvar.

O servidor de host usa o novo fuso-horário. Quando o servidor exibe um ticket, a Hora inicial reflete o fuso-horário do servidor.

Para criar um tipo de serviço

1. Na guia Administração, selecione Tipos de serviço.

   A lista de Tipos de serviço aparece.

2. Clique em Resolução de prioridade 1 ou outro Tipo de serviço que gerencie Solicitações de prioridade 1.

   A página Atualizar tipo de serviço é exibida.

3. Marque a caixa de seleção Usar fuso-horário do usuário final.
4. Clique em Salvar.

   O registro Tipo de serviço é atualizado.

Para exibir os fusos-horários no ticket

1. Em outro computador, abra um ticket de Solicitação e defina a Prioridade como 1.

   Observação: se você está usando Metas de serviço, defina os valores no ticket para fazer a meta usar Resolução de Prioridade 1.

2. Exiba o ticket e clique na guia Tipo de serviço.

   A hora inicial reflete o fuso-horário do servidor. A Hora de expiração reflete a hora no computador local do usuário final.

3. Feche a página que exibe o ticket de Solicitação.
4. Altere o fuso-horário no computador local do usuário final.
5. Exibir o Tipo de serviço do ticket no computador local do usuário final para ver os valores de Hora de expiração correspondentes com base no fuso-horário do usuário.

   A Hora de expiração reflete o novo fuso-horário.

Observação: para obter informações detalhadas sobre Tipos de servidor ou Código de servidor, consulte a *Ajuda online*.

Configurar turnos de trabalho

Os turnos de trabalho identificam os dias, datas e horas em que um evento ou agendamento está em vigor. Você pode especificar dias, datas ou ambos. Especificar um horário é opcional.

Observação: para obter informações sobre como definir turnos de trabalho, consulte a *Ajuda online*.

Ao monitorar eventos de tickets, os turnos de trabalho definem quando o evento é monitorado ou, em outras palavras, quando as horas contam. Por exemplo, ao usar o evento predefinido "P1 ativo - Notif destin ocorr.", se uma ocorrência de prioridade 1 for aberta às 16:45 e o horário do turno de trabalho for das 9:00 às 17:00, o evento monitorado enviará automaticamente uma notificação ao destinatário da ocorrência às 9:45 do dia seguinte.

Observação: os turnos de trabalho também são usados para atribuir automaticamente tickets a contatos.

Mais informações:

Estabelecendo estrutura de suporte (na página 289)

Segurança

Antes de permitir que funcionários usem o CA SDM, é importante configurar a segurança para determinar o seguinte:

- Quais usuários podem acessar o sistema.
- Qual nível ou níveis de acesso os usuários podem ter.
- Como os usuários são autenticados quando efetuam logon.

Observação: para obter detalhes sobre como realizar tarefas de administração de segurança, consulte a *Ajuda online*.

Configurações da base de usuários CA EEM e CA Workflow

O CA EEM é um repositório central de informações de usuário (identidades). O CA EEM define a autenticação do usuário e o acesso a outros aplicativos. Se você tiver vários produtos CA Technologies instalados, é possível que alguns possam usar o CA EEM para armazenar identidades e políticas de acesso. O CA SDM usa apenas o CA EEM para autenticação. O CA EEM não é uma opção de configuração do CA SDM e deve ser instalado separadamente.

O repositório de registros de usuário do CA EEM é *qualquer uma* das origens a seguir:

- Um diretório LDAP externo.
- Suas próprias tabelas internas no MDB

O CA EEM tem uma interface LDAP que é usada quando ele é configurado para usar o MDB.

Observação: as tabelas do MDB usadas pelo CA EEM são diferentes daquelas usadas pelo CA SDM.

Se sua organização usar um servidor de diretório, como o Active Directory ou o eTrust Directory, considere configurar o CA EEM para usar o diretório de sua base de usuários. Essa configuração torna os usuários em seu diretório acessíveis por qualquer outro aplicativo que use o CA EEM. Como o CA EEM centraliza o gerenciamento do acesso, em geral ele é instalado em um único servidor.

Observação: para obter mais informações sobre a instalação, consulte o *Guia de Implementação*.

CA Workflow

Durante a instalação do CA SDM, é possível opcionalmente instalar o CA Workflow, um mecanismo de fluxo de trabalho integrado. Como o CA Workflow usa o CA EEM para todas as informações de usuário, o CA EEM gerencia todas as tentativas de autenticação e determinadas permissões. O CA Workflow não tem nenhum conhecimento dos registros de contatos do CA SDM.

Observação: para obter informações sobre como configurar o acesso ao CA Workflow, consulte o *Guia de Implementação*.

CA SDM

O CA SDM armazena informações de contato nas tabelas do MDB. Essas tabelas não têm um relacionamento com o CA EEM. O CA SDM não usa o CA EEM para o gerenciamento de acesso ou identidade. O CA SDM gerencia seu próprio acesso e segurança usando Tipos de acesso e Partições de dados.

O CA SDM usa o CA EEM apenas para autenticação. Se quiser usar o CA EEM para autenticar usuários no CA SDM, instale o CA EEM. Se você integrar o CA SDM com o CA EEM, ele substitui a autenticação do sistema operacional do CA SDM com a autenticação do CA EEM.

Observação: para obter informações sobre como instalar o CA EEM, consulte o *Guia de Implementação*. Para integrar o CA EEM e o CA SDM, é preciso definir as opções *eiam_hostname*, *use_eiam_artifact*, e *use_eiam_authentication* no Gerenciador de opções, Segurança. Para obter mais informações sobre essas opções, consulte a *Ajuda online*.

A base de usuários do CA SDM é separada da base do CA EEM e, portanto, separada da base de usuários do CA Workflow. A vantagem disso para o CA Workflow é que itens de fluxo de trabalho podem ser atribuídos a e concluídos por indivíduos externos ao CA SDM. Isso é útil quando o CA EEM aponta para o servidor LDAP de sua organização.

O desafio está na integração com o CA SDM. Um item de trabalho não pode ser atribuído diretamente ao registro de contato do CA SDM em si. A atribuição do item de trabalho a contatos do CA SDM pode ser feita somente se ambas as condições abaixo forem satisfeitas:

- O contato do CA SDM tem um registro correspondente no CA EEM
- Esses registros tenham IDs de usuário correspondentes.

Para resumir:

- O CA SDM usa o MDB para armazenar informações de Contato. O CA SDM também conta com a integração de LDAP, o que permite criar novos Contatos a partir de um servidor LDAP, e sincronizar contatos existentes com o diretório.
- O CA EEM é a solução da CA para gerenciamento centralizado de usuários. Se você tem vários produtos da CA instalados, é possível que todos eles estejam usando o CA EEM para armazenar identidades e políticas de acesso.

- O CA EEM pode ser configurado para apontar para um diretório externo (LDAP) ou usar o MDB para armazenar informações de usuários. O próprio CA EEM tem uma interface LDAP que é usada quando ele é configurado para usar o MDB.

  Observação: as tabelas usadas pelo CA EEM no MDB são diferentes das usadas pelo CA SDM.

- O CA Workflow sempre usa o CA EEM para armazenar informações de usuário e autenticação. Os itens de trabalho podem ser atribuídos apenas a usuários conhecidos pelo CA EEM, e somente os usuários definidos pelo CA EEM podem acessar a interface web do usuário da lista de trabalho e do IDE do CA Workflow.

As informações a seguir discutem várias opções de configuração dos produtos e como elas afetam a integração entre o CA SDM e o CA Workflow. Selecione a configuração que melhor corresponda ao seu uso do CA Workflow e (opcionalmente) um servidor de diretório LDAP.

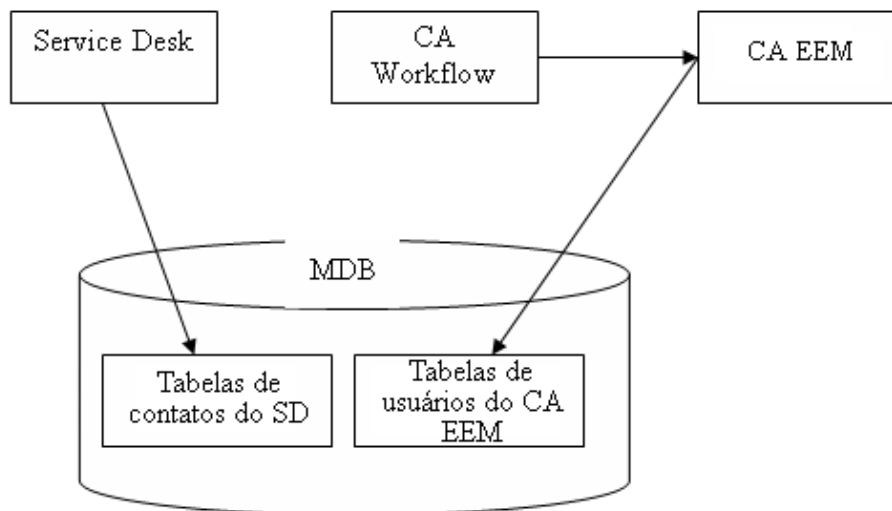
Mais informações:

Configurações da base de usuários CA EEM e CA Workflow (na página 186)
O CA EEM como configuração de LDAP (na página 191)

Configuração padrão

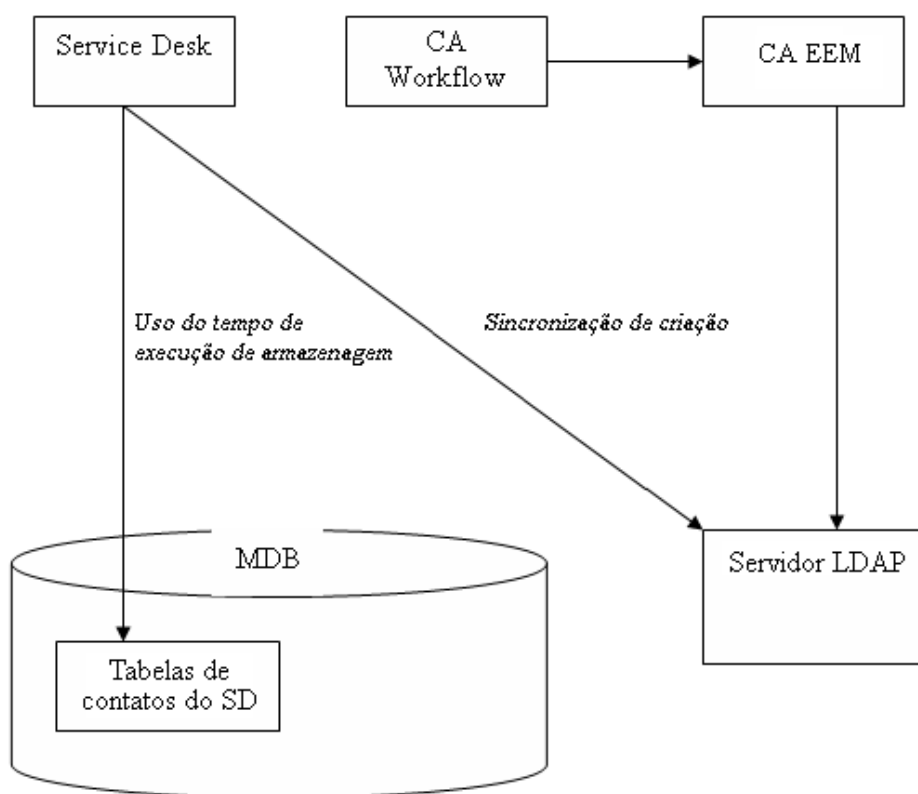
O CA SDM e o CA Workflow armazenam informações de usuário depois de uma instalação padrão, conforme abaixo:

- O CA SDM armazena informações de usuário nas tabelas de Contato do CA SDM no MDB.
- O CA Workflow usa o CA EEM para armazenar informações de usuário nas tabelas de Usuário do CA EEM no MDB.

O diagrama seguinte ilustra onde os produtos armazenam informações de usuário:

Considere usar a configuração padrão se seu local usa pouco ou não usa o CA Workflow ou um servidor de diretório LDAP. Esta configuração pode apresentar alguns desafios. Cada usuário do CA Workflow requer um registro de usuário no CA EEM.

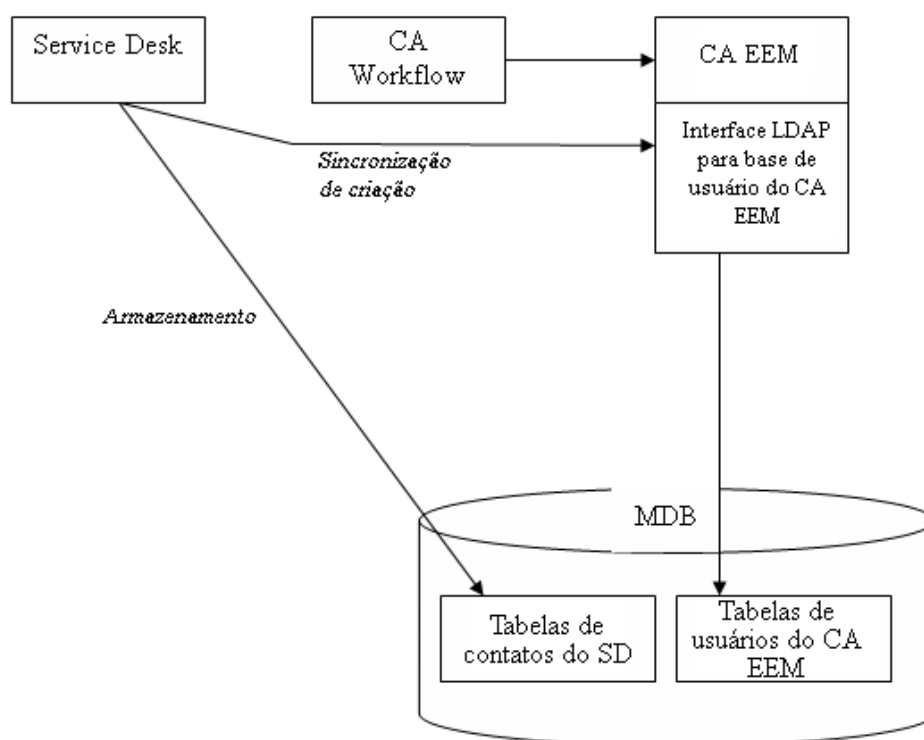
Configuração de servidores LDAP externos

A administração de contatos é simplificada se o CA SDM e o CA Workflow usarem o mesmo servidor de diretório LDAP. Isso é especialmente útil quando sua empresa já usa um servidor LDAP como o diretório principal para usuários. Usando os recursos LDAP do CA SDM, as IDs de usuário de registros de contato correspondem àquelas no diretório, permitindo a fácil atribuição de itens de trabalho a analistas do CA SDM. As integrações tornam-se ainda mais fáceis quando o CA SDM usa o CA EEM para autenticação.

O diagrama a seguir mostra um cenário no qual todos os usuários do diretório LDAP automaticamente têm acesso à lista de trabalho da aplicação da Web do CA Workflow. O CA SDM ainda usa as tabelas de contatos no MDB para seus registros de usuário, porém esses podem ser importados do e sincronizados com o servidor LDAP.

Mais informações:

Dados no diretório LDAP (na página 222)

O CA EEM como configuração de LDAP

Quando o CA EEM é configurado para usar o MDB em vez de um diretório externo para armazenar informações de usuário, o CA EEM expõe o diretório de usuários usando uma interface LDAP. Se sua empresa não usa um servidor LDAP externo, você ainda pode usufruir das vantagens da configuração de LDAP externo ao configurar o CA SDM para usar o CA EEM como uma origem LDAP. Essa configuração pode ser útil se sua empresa não usar um servidor LDAP, porém deseja consolidar o gerenciamento de usuários no CA EEM. Outros produtos CA também usam o CA EEM, que pode simplificar significativamente o gerenciamento de usuários.

Observação: esta configuração se aplica somente quando o CA EEM estiver configurado para usar o MDB. Se o CA EEM estiver configurado para usar um servidor LDAP externo, configure o CA SDM para apontar para o mesmo servidor LDAP, e *não* para o CA EEM.

Atualização

Se você estiver migrando de uma versão anterior do CA SDM ou fazendo o carregamento em lote de muitos registros de contato, terá que adicionar manualmente esses usuários ao CA EEM para que eles consigam acessar o CA Workflow.

Configurar o armazenamento de usuário do CA EEM r8.4 SP4 CR05.

É possível configurar o CA EEM r8.4 SP4 CR05 para armazenar registros do usuário em um diretório LDAP externo ou em suas próprias tabelas MDB internas. Quando o CA EEM usa um diretório LDAP externo, ele é uma interface somente leitura; você não pode adicionar nem modificar usuários pela interface do CA EEM.

Siga estas etapas:

1. Selecione Iniciar, Programas, CA, Embedded Entitlements Manager, EEM UI.

   A interface do usuário do CA EEM aparece.

2. Clique na guia Configurar.
3. Clique na subguia EEM Server.
4. Na seção esquerda, clique no link Usuários globais/Grupos globais.
5. Na seção direita, selecione uma das seguintes opções:
   - Armazenar no armazenamento de dados interno
   - Referência de um diretório externo
   - Referência do CA SiteMinder

     Observação: se você selecionar a Referência de uma opção de diretório externa, será solicitado a fornecer os detalhes do servidor LDAP.

6. Clique em Salvar.

   A configuração do armazenamento de usuários para o CA EEM está completa.

   Observação: para obter mais informações sobre o CA EEM, consulte a *Ajuda online do CA EEM*.

Configurar o armazenamento de usuários do CA EEM r12 CR02

É possível configurar o CA EEM r12 CR02 para armazenar registros do usuário em um diretório LDAP externo ou em suas próprias tabelas MDB internas. Quando o CA EEM usa um diretório LDAP externo, ele é uma interface somente leitura; você não pode adicionar nem modificar usuários pela interface do CA EEM.

Siga estas etapas:

1. Selecione Iniciar, Programas, CA, Embedded Entitlements Manager, Admin UI.

   A interface do usuário do CA EEM aparece.

2. Clique na guia Configurar.
3. Clique na subguia Armazenamento de usuário.
4. No painel do lado esquerdo, clique no link de Armazenamento do usuário.
5. Na seção direita, selecione uma das seguintes opções:
   - Armazenar no armazenamento interno do usuário
   - Referência de um diretório LDAP externo.
   - Referência do CA SiteMinder

     Observação: se você selecionar a Referência de uma opção de diretório externa, será solicitado a fornecer os detalhes do servidor LDAP.

6. Clique em Salvar.

   A configuração do armazenamento de usuários para o CA EEM está completa.

   Observação: para obter mais informações sobre o CA EEM, consulte a *Ajuda online do CA EEM*.

Adicionar usuários e grupos

Se o CA EEM estiver configurado para fazer referência a um diretório externo, não é possível adicionar usuários pela interface de usuário do CA EEM. O CA EEM é uma interface somente leitura do servidor LDAP. Você deve usar a interface fornecida com seu produto de servidor LDAP para atualizar os registros de usuário.

Para adicionar um novo registro de usuário

1. Clique em Iniciar, Programas, CA, Embedded Entitlements Manager, Admin UI/EEM UI.
2. Efetue logon usando o nome de usuário e a senha do CA EEM. Essas informações são especificadas durante a instalação do CA EEM. O CA EEM deve ser instalado separadamente e não é uma opção de configuração para o CA SDM.
3. Clique na guia Gerenciar identidades.
4. Na seção esquerda, clique na guia Usuários para pesquisar e atualizar registros de usuários existentes.

   Observação: para gerenciar grupos do CA EEM, clique na guia Grupos.
5. Clique no ícone à esquerda da pasta Usuários.

   O formulário para criação de um registro de usuário aparece.
6. Preencha o formulário e clique em Salvar.

   O novo registro de usuário do CA EEM é salvo no MDB.

Observação: as etapas para editar um registro de usuário existente e manter registros de grupo são semelhantes a estas etapas. Para obter mais informações, consulte a *Ajuda online do CA EEM*.

Configurar acesso ao CA Workflow no CA EEM

Todos os logons em CA Workflow são autenticados por CA EEM. Uma pessoa deve ter um registro de usuário do CA EEM para acessar o aplicativo IDE ou Lista de trabalho do CA Workflow. O administrador do CA Workflow, especificado durante a configuração do CA SDM, tem acesso completo.

Por padrão, este usuário é usado por CA SDM para a integração de Workflow. Esta conta de usuário é definida pelas opções cawf_username e cawf_password em Gerenciador de opções. Você deve certificar-se de que o nome de usuário e senha definidos nessas opções estejam corretos e de que o usuário tenha acesso completo aos recursos do CA Workflow no CA EEM.

O CA Workflow também usa o CA EEM para restringir o acesso a funções específicas do CA Workflow. Esse acesso é controlado por duas Classes de recursos chamadas IDE e Processo:

- O recurso IDE tem uma única ação chamada *login*, que dá acesso de logon ao IDE. Um usuário deve ter permissão para esta ação para efetuar o logon no aplicativo IDE do CA Workflow.
- O recurso Processo tem uma única ação chamada *start,* que fornece a capacidade de iniciar uma instância de processo. O usuário deve ter permissão para esta ação para iniciar processos de dentro do aplicativo da Web de lista de trabalho.

Observação: todos os usuários conhecidos do CA EEM têm acesso ao aplicativo Lista de trabalho do CA Workflow para exibir e executar tarefas de itens de trabalho. Essa permissão só está disponível para iniciar novas instâncias da Lista de trabalho. Estas classes de recurso são definidas com a instância do aplicativo CA SDM no CA EEM; ao efetuar logon na interface de usuário da Web do CA EEM, você precisa especificar a instância do aplicativo CA SDM para ver os recursos, as políticas e grupos discutidos aqui.

Os usuários que necessitam fazer logon ao IDE ou iniciar instâncias de processo devem obter autorização de acesso aos recursos e ações descritos acima. A configuração do CA SDM adiciona duas diretivas ao CA EEM que concedem acesso a estes recursos. Por conveniência, as diretivas concedem o acesso a dois grupos na sua instância de aplicativo: Administradores de Workflow e Iniciadores de processos de Workflow. Você pode simplesmente adicionar usuários ao grupo Administradores de workflow para que eles obtenham acesso ao IDE. Adicionar usuários ao grupo de iniciadores de processo de fluxo de trabalho permitirá a eles iniciar processos do aplicativo Lista de trabalho.

Para adicionar ou remover usuários dos grupos mencionados acima:

1. Faça logon na IU da Web do CA EEM
2. Na página de logon, selecione o aplicativo CA SDM e especifique o nome e senha de administrador do CA EEM.
3. Na página principal do CA EEM, selecione Gerenciar identidades.
4. Selecione Pesquisa de usuários, digite o critério de pesquisa e execute a pesquisa.

5. Selecione um usuário na lista de resultados.
6. Na exibição de detalhes do usuário, adicione ou remova a participação em grupo na seção de participação em grupo do aplicativo.

   Observação: se essa seção não for exibida, talvez seja necessário pressionar o botão Adicionar detalhes de usuário de aplicativo.
7. Ao terminar, pressione Salvar.

   O usuário será adicionado ou removido, conforme aplicável.

Atribuição de item de trabalho do CA Workflow

A Função de um item de trabalho do CA Workflow pode ser atribuída a agentes humanos ou não humanos. Exemplos de agentes não humanos podem incluir um objeto Java personalizado, um processo de linha de comando ou outra instância de processo do CA Workflow. No caso de agentes humanos, a função do item de trabalho é definida com a Lista de usuários global, que é o repositório de usuários do CA EEM. Essa deve ser uma lista separada por ponto-e-vírgula de IDs de usuário. Por exemplo:

```
ServiceDesk; abeju01; Meu Grupo
```

atribui o item de trabalho à Central de serviços de usuários, abeju01 e a qualquer um que pertença a Meu Grupo. Isso significa que qualquer um desses usuários pode concluir o item de trabalho.

Observação: todos esses usuários e grupos devem ser conhecidos pelo CA EEM. Portanto, o grupo Meu Grupo é um grupo no CA EEM, e não um grupo no CA SDM.

Para atribuir dinamicamente um item de trabalho a um único usuário, defina a lista de usuários (userlist) da Função como $MeuUsuário.

Observação: NÃO adicione aspas duplas à seqüência de caracteres.

Declare um atributo de seqüência de caracteres chamado MeuUsuário na definição do processo. Quando o item de trabalho for criado, o valor em MeuUsuário será usado para a atribuição de item de trabalho. Isso significa que você deve designar um valor válido a MeuUsuário: um único nome de usuário ou uma lista de nomes de usuário separados por ponto-e-vírgula. Essa atribuição deve ser feita antes que seja usado com um item de trabalho.

Um exemplo de atribuição de ID de usuário a variáveis pode ser visto na demonstração de definição de requisição de PC. Ela pressupõe que a ID de usuário de um registro de Contato do CA SDM corresponde à ID de usuário de um registro de usuário correspondente no CA EEM. A demonstração de requisição de PC mostra como recuperar IDs do usuário do CA SDM usando a interface de serviço web. As IDs do usuário podem se originar do ticket (como o destinatário, destinatário de categoria etc.)

Para resumir a configuração da atribuição de um item de trabalho:

1. Inicie o IDE do CA Workflow.
2. Clique duas vezes na Definição de processo que deseja editar.

   A Definição de processo é exibida na janela Designer de processo
3. Selecione a guia Funções
4. Adicione ou atualize uma função.
5. Selecione a Lista de usuários globais na lista de Agentes disponíveis e clique em Editar.
6. Insira uma lista das IDs de usuário do CA EEM separadas por ponto-e-vírgula. Você pode usar o botão Procurar para navegar e selecionar usuários conhecidos do CA EEM.

Considerações de segurança

Quando você instala o CA SDM pela primeira vez, o sistema está configurado para permitir o acesso máximo a qualquer contato que não tenha um tipo de acesso explícito definido em seu registro de contato. Talvez deseje fazer modificações adicionais à implementação de segurança predefinida. No mínimo, você deverá realizar as seguintes etapas antes de permitir que as pessoas trabalhem com o aplicativo:

1. Revise os tipos de acesso predefinidos para determinar um padrão razoável para seu sistema.

   O tipo de acesso do administrador está definido como o valor padrão, o que não é uma escolha adequada para a maioria dos sites. Por exemplo, alguns sites oferecem acesso somente leitura ao CA para a maioria dos membros da organização de TI. Caso defina Usuário do CMDB como o tipo de acesso padrão, não é necessário definir o tipo de acesso de novos usuários, a menos que eles precisem de privilégios adicionais. Analogamente, se a maioria dos usuários precisar do privilégio para gravar informações de configuração, é possível selecionar Analista do CMDB como o tipo de acesso padrão.

2. Atribua os tipos de acesso dos contatos restantes de forma explícita.

   Por exemplo, caso tenha escolhido Usuário do CMDB como o tipo de acesso padrão, modifique os registros dos contatos de seus analistas para atribuir um tipo de acesso de analista.

Observação: para obter mais informações, consulte a .*Ajuda online*.

Autenticação CA EEM para o CA Process Automation

O CA SDM e o CA Process Automation comunicam-se usando uma troca de serviços web sobre HTTP. Embora tenham sido tomadas todas as medidas para enviar quantidades mínimas de informações sensíveis entre os produtos, uma entidade maliciosa pode acessar nomes de usuário, senhas e informações proprietárias. Você pode seguir etapas deliberadas para proteger a comunicação do servidor.

Para autenticação do CA Process Automation, considere as seguintes recomendações:

- Como uma opção, é possível configurar o CA Process Automation para usar o CA EEM como um servidor de autenticação. O CA Process Automation implementa grupos e políticas padrão no CA EEM. Você pode modificar os grupos e políticas padrão para atender as necessidades da organização.
- Usar CA EEM elimina a necessidade de enviar nomes e senhas de usuário em texto sem formatação para fins de autenticação. Se você está usando multilocação, CA EEM é exigido para ativar multilocação no CA Process Automation.

  Observação: para obter segurança de autenticação nesta integração, não é necessário ter o CA SDM configurado para usar o CA EEM. Porém, o CA EEM é exigido para implementação de multilocação do CA Process Automation. Para informações sobre implementação de multilocação com o CA Process Automation, consulte a documentação do guia do usuário do CA Process Automation. Para informações sobre a configuração do CA Process Automation para usar o CA EEM como um servidor de autenticação, consulte a documentação de instalação e configuração do CA Process Automation.

- Configure CA Process Automation para comunicar usando comunicações seguras em HTTPS. HTTPS URLs usa SSL/TLS para eliminar trocas de texto sem formatação ao proteger dados proprietários e outros dados sensíveis contra revelação maliciosa ou acidental.

  Observação: para obter informações sobre como configurar CA Process Automation para usar HTTPS, consulte a documentação de instalação e configuração de CA Process Automation.

Autenticação de usuário

O CA SDM fornece uma solução de autenticação de usuário que você pode personalizar como parte do tipo de acesso. A mesma autenticação é usada por todas as interfaces do CA SDM e por outros produtos CA.

Observação: é possível configurar a autenticação de usuários do CA SDM em um computador separado, se necessário. Consulte o *Guia de Implementação* para obter mais informações.

A autenticação é flexível, permitindo tirar proveito de mecanismos de autenticação externos, como Windows, validação de usuário HTTPD ou autenticação LDAP. Você também pode selecionar entre diversas opções internas de autenticação, incluindo senha do sistema operacional, PIN, acesso de usuário convidado ou nenhum acesso.

Como o CA SDM autentica usuários

O CA SDM autentica usuários com base na ID de usuário definida em seu registro de contato. O produto também faz o seguinte quando um usuário solicita acesso ao sistema:

1. Se uma ID de usuário externa estiver disponível (da validação HTTPD ou Windows), o CA SDM vai procurar o contato por ID de logon. Se o contato for localizado e possuir um tipo de acesso que permita a autenticação externa, o usuário terá permissão para acessar o produto.
2. Se a autenticação externa não for bem-sucedida, o CA SDM solicitará ao usuário uma ID de usuário e senha. O produto procura um registro de contato para a ID de usuário, obtém o tipo de acesso e, em seguida, autentica o usuário como especificado pelo tipo de acesso.

Em muitas instalações, os tipos de acesso predefinidos fornecem uma autenticação razoável para esse tipo de usuário; no entanto, em alguns casos convém modificar as informações de autenticação para um tipo de acesso predefinido ou definir um novo tipo de acesso para lidar com um método diferente de autenticação no caso de alguns usuários. Você deve revisar as configurações de autenticação para os tipos de acesso predefinidos para determinar se atendem a suas necessidades, ou se necessita modificá-los ou definir tipos adicionais.

Autenticação externa

O CA SDM permite aos usuários acessar o sistema sem fornecer uma ID de usuário desde que as três condições seguintes sejam atendidas:

- A autenticação externa está definida para o usuário.
- A ID de usuário autenticada externamente está associada a um contato em sua tabela de contatos.
- O registro de contato tem um tipo de acesso cuja definição de autenticação permite autenticação externa.

A autenticação externa não permite que os usuários acessem o sistema nos seguintes casos:

- Um usuário tenta acessar através de um servidor não seguro.
- Um usuário tenta acessar, mas está atribuído a um tipo de acesso que não permite autenticação externa.

Nenhum dos tipos de acesso predefinidos usa autenticação externa. Se desejar usar autenticação externa para os usuários, considere modificar os tipos de acesso de funcionário, analista e administrador para definir autenticação externa. Os requisitos individuais de seu site e os diferentes tipos de usuários determinarão se você deverá permitir a autenticação externa. Quando a autenticação externa é usada, a configuração de servidor controla o acesso a arquivos e diretórios. Ao definir autenticação para um tipo de acesso, é possível decidir seu uso da seguinte forma:

- Não use autenticação externa que já esteja implementada, como logon de usuário do Windows ou validação pelo servidor de HTTPD.
- Use a autenticação que está implementada e permita ou negue o acesso com base nela.

Observação: se a autenticação externa não for permitida, o usuário é autenticado com base no tipo de validação que você especificar.

Abaixo estão alguns exemplos de autenticação externa:

- Se um usuário que tenha acesso de administrador faz o logon em um computador Windows, ele poderá realizar tarefas administrativas sem informar novamente nenhuma informação de logon.
- Se um usuário tiver validação no servidor de HTTPD, poderá acessar a interface da web sem informar novamente nenhuma informação de logon. Como o tipo de acesso de administrador especifica o tipo de usuário web do analista, a interface da web apropriada ao analista será apresentada automaticamente.

Tipos de validação

Os tipos de validação autenticam usuários apenas sob as seguintes circunstâncias:

- O tipo de acesso do usuário não permite a autenticação externa.
- O tipo de acesso do usuário permite a autenticação externa, mas o usuário não foi validado externamente (por exemplo, o usuário pode ter tentado o acesso por um servidor não-seguro).

O CA SDM fornece as seguintes opções de validação:

- **Sem acesso** — Os usuários deste tipo não têm nenhum acesso, a menos que a autenticação externa seja permitida e válida.
- **Aberto** — Os usuários com esse tipo têm acesso, sem nenhuma autenticação adicional necessária.
  - **SO** — Os usuários deste tipo inserem sua senha do sistema operacional para acesso. O sistema operacional usado para validação é o que está em execução no Host de validação de usuários. Essa opção é a validação padrão dos tipos de acesso de administrador, analista e funcionário.

    Observação: para obter mais informações sobre o Host de validação de usuários, consulte o *Guia de Implementação*.

- **PIN** — Os usuários com esse tipo de acesso obtêm acesso ao digitar o valor correto do campo PIN em seu registro de contato como sua senha. Para definir o campo PIN, digite o nome de atributo do campo ao selecionar o PIN como o tipo de validação. O PIN é o tipo de validação padrão para o tipo de acesso de cliente, que usa o valor no campo ID do cliente (contact_num) como o PIN.

  Observação: para obter uma lista de nomes do atributo para o objeto cnt, que é o objeto definido para a tabela de contatos, consulte o *Guia de Referência Técnica*.

Contagens de usuários conectados e usuários licenciados

O Indicador Principal de Desempenho webLicenseCt conta o número de usuários conectados que estão usando uma licença do CA SDM. O Licenciado? Caixa de seleção na página de Tipo de acesso que determina se este contato é um tipo de acesso licenciado. Os contatos atribuídos a tipos de acesso não licenciados só podem exibir ou atualizar os próprios dados pessoais. Além disso, o KPI webSessionCt conta o número total de sessões web—tanto os usuários de analistas licenciados como os usuários finais fazendo logon na interface de autoatendimento web são todos contados. Se um usuário fizer logon várias vezes no CA SDM, seja em seu computador ou em outro computador, ocorrem várias sessões web. Se o usuário for um analista, são usadas várias licenças. Várias páginas abertas para o usuário conectado não afetam a contagem de sessão web e licença web.

Observação: para obter mais informações sobre tipos de contato, consulte a *Ajuda online*.

Exemplo: contadores de usuários licenciados e conectados

Três usuários finais estão conectados na interface de autoatendimento web e analisando alguns anúncios.

Ao mesmo tempo, cinco analistas licenciados (que possuem um ticket de caixa de seleção em seu tipo de acesso) estão conectados na interface do analista e trabalhando em incidentes.

O KPI webLicenseCt mostra uma contagem de cinco, que significa que estão sendo usadas atualmente cinco licenças.

O KPI webSessionCt mostra uma contagem de oito, que significa que oito usuários no total estão conectados à interface da web do CA SDM.

Logs internos

Você pode definir se um tipo de acesso particular será capaz de exibir logs internos. Se for permitido exibir logs internos, os contatos verão uma caixa de seleção chamada Interno em cada uma das janelas de Log de atividades, que poderão selecionar para marcar a atividade como interna. Quando atividades são marcadas como internas, apenas os contatos com um tipo de acesso qualificado para exibir logs internos verão a atividade ou serão notificados sobre ela.

Integração do CA SDM

O tipo de acesso também identifica o tipo de usuário que faz contato com esse tipo de acesso ao usar outros produtos CA com o CA SDM. Quando um contato com esse tipo de acesso usa outro produto, seus direitos de usuário a esse produto são determinados pelos valores que você especificou para o tipo de acesso.

Associações de partições de dados

Partições de dados podem ser atribuídas a contatos individuais, mas o método preferencial é atribuir partições de dados com base no tipo de acesso. Após associar partições de dados a diferentes tipos de acesso, você pode associar um contato a um tipo de acesso específico e definir sua partição de dados. O tipo de acesso tem uma opção específica para substituir a partição de dados dos contatos.

Para associar uma partição de dados a um tipo de acesso, você define partições de dados que sejam significativas para seu local e, a seguir, seleciona uma das partições de dados ao definir ou modificar um tipo de acesso.

Importante: Outras configurações de segurança do CA SDM podem ter prioridade sobre a partição de dados.

Partições de dados

Uma partição de dados é um subconjunto de um banco de dados do CA SDM que controla o acesso do usuário a tickets e outros registros de dados com base em seu conteúdo. Por exemplo, é possível restringir a visualização de um usuário do banco de dados apenas para os itens de configuração atribuídos à organização do usuário. Além disso, você pode restringir um usuário a atualizar apenas tickets atribuídos e permitir o acesso- somente leitura a outros itens de configuração.

Uma partição de dados consiste em um conjunto padrão de restrições. A restrições de partição de dados identificam a tabela que está sendo controlada pela partição de dados e o tipo de restrição. Os tipos de restrição especificam o que o usuário pode fazer, tal como criar, excluir, atualizar, exibir etc, na partição de dados. Depois de atribuir uma partição de dados a um tipo de acesso, o qual por sua vez é atribuído a um registro de contato do usuário, as restrições e os tipos de restrição controlarão o acesso do usuário aos registros na tabela de banco de dados do CA SDM.

Você também pode exibir restrições independentemente da partição de dados que as utilizam. Por exemplo, você pode exibir todas as restrições de uma tabela específica independente de partição de dados.

Observação: para obter mais informações sobre como usar restrições de partição de dados, consulte a *Ajuda online*.

Configuração da partição de dados

Você pode definir um número ilimitado de partições de dados. Cada partição de dados consiste em um conjunto de restrições e validações relacionados a cada tabela de banco de dados restrita à partição de dados. Para cada tabela em uma partição de dados, você pode especificar autorizações independentes para exibir, atualizar, criar ou excluir registros, usando critérios especificados em um formato semelhante a uma cláusula Where de SQL. Você pode basear a restrição em qualquer atributo do registro sendo acessado, combinado a qualquer dado no registro de contato do usuário. Isso permite uma flexibilidade considerável ao definir partições de dados. Por exemplo, usar o campo de Fornecedor na tabela Contact permite que restrições de partição de dados sejam definidas para fornecedores com acesso direto ao CA SDM.

por razões de desempenho, o CA SDM não permite que uma restrição de partição de dados contenha uma união Cartesiana. Uma união Cartesiana resulta de uma restrição contendo um "OU" que restringe completamente todas as tabelas unidas pelo operador OU. Para assegurar-se de que sua restrição de partição de dados não produza uma união Cartesiana, digite o seguinte comando:

Windows

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

UNIX

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

Importante: Quaisquer partições de dados que sejam recuperadas por esse programa deverão ser atualizadas apropriadamente. Para obter mais informações sobre como definir partições de dados, restrições e tipos de restrições, consulte a *Ajuda online*.

Especificações da restrição

Especifique restrições e testes de validação no Majic usando a metalinguagem de definição de objetos.

Observação: para obter informações, consulte o *Guia de Referência Técnica*.

As restrições definidas em Majic são muito similares a uma cláusula Where de SQL, com as seguintes exceções:

- Os nomes de atributos na restrição são nomes de atributos de objetos, não o nome do atributo do banco de dados do esquema.
- Você pode fazer referência ao valor de um atributo no registro de contato do- usuário conectado usando um nome no seguinte formato, onde *att_name* é o nome Majic do atributo desejado:

  ```
  @root.att_name
  ```

  Por exemplo, ao especificar @root.location você faz referência à ID de local do contato atual.

  As uniões são especificadas usando o seguinte formato, onde *foreign-key* é o nome Majic do atributo SREL na tabela para a qual você está gravando a restrição de partição de dados, e *attribute-in-referenced-table* é o nome Majic do atributo na tabela sendo unida:

  ```
  foreign-key.attribute-in-referenced-table
  ```

Por exemplo, para fazer referência ao fornecedor de manutenção do ativo associado a um relatório de incidente, especifique:

```
resource.vendor_repair
```

Essa especificação é recursiva. Por exemplo, você pode fazer referência ao nome do fornecedor usando:

```
resource.vendor_repair.name
```

A tabela a seguir contém exemplos de restrições válidas para o uso com a tabela Change_Request, usada para armazenar informações de requisição de mudança:

Tipo de restrição	Código e descrição
Exibir	organização.destinatário = @raiz.organização Especifica que o usuário pode exibir apenas requisições de mudança nas quais a organização do destinatário é a mesma que a organização do usuário.
Pré-atualizar	requestor = @root.id Especifica que o usuário pode apenas atualizar as requisições de mudança nas quais ele é o chamador ou solicitante.

No entanto, não é possível gravar uma restrição que use a união em ambos os lados da expressão, como mostra o seguinte exemplo:

```
assignee.org = requestor.org
```

Tipos de restrição

Você pode atribuir os seguintes tipos de restrições para cada tabela controlada em uma partição de dados:

Criar

Especifica os critérios que devem ser atendidos antes de criar um registro. Quando um usuário na partição de dados tenta criar um registro que não corresponde à condição de teste de criação, o CA SDM exibe a mensagem de erro associada à restrição e não salva o registro.

Padrões

Especifica uma ou mais declarações de atribuição, separadas por ponto-e-vírgula, que definem valores a serem atribuídos a campos em branco em um novo registro no momento em que esse registro é armazenado. A sintaxe de cada instrução de atribuição é, em que att_name é o nome de um atributo Majic do registro e value pode ser um número inteiro, uma seqüência de caracteres entre aspas ou uma referência no formato @root.att_name a um atributo Majic no registro de contatos do usuário atual:

nome_atributo=valor

No caso de tabelas atualizadas para tickets, valores padrão são colocados no registro no momento em que esse é exibido, e são mostrados na exibição inicial de um novo registro. Você pode atribuir um valor padrão a um campo de referência (um SREL do Majic) ao inseri-lo no código com o formato de uma ID persistente. Uma ID persistente é um nome de objeto seguido por dois-pontos e uma ID de número inteiro. Por exemplo, você pode definir um valor padrão para a categoria ao incluir o seguinte na especificação de padrão, em que PCAT é o alvo do SREL (como mostra o arquivo Majic) e 12345 é o número de ID da categoria desejada:

```
category='PCAT:12345'
```

Você pode listar ID persistentes para um objeto usando um comando com o seguinte formato:

```
bop_odump domsrvr pcat "" sym
```

Excluir

Especifica os critérios que devem ser atendidos antes de excluir um registro. Quando um usuário na partição de dados tenta excluir um registro que não corresponde à condição de exclusão, o CA SDM exibe a mensagem de erro associada à restrição e não exclui o registro.

Pré-atualizar

Especifica os registros na tabela controlada que um usuário pode atualizar na partição de dados. Quando um usuário na partição de dados solicita um registro que não corresponde à condição de pré-atualização, o CA SDM torna o registro somente leitura e exibe a mensagem de erro associada à restrição.

Atualizar

Especifica os critérios que devem ser atendidos quando um registro é salvo. Quando um usuário na partição de dados tenta salvar um registro que não corresponde à condição de teste de atualização, o CA SDM exibe a mensagem de erro associada à restrição e não salva o registro.

Exibir

Especifica os registros na tabela controlada que um usuário pode exibir na partição de dados. Essa restrição é automaticamente aplicada a todas as listas selecionadas por um usuário nessa partição de dados, além de qualquer critério de seleção explicitamente especificado pelo usuário.

A exibição pode incluir uniões com outras tabelas e referências no formato @root.*att_name* a atributos Majic no registro de contato do usuário conectado. Exemplos válidos são:

```
requestor.organization = @root.organization

requestor.organization.name = 'MIS'

assignee = @root.id

organização.destinatário = @raiz.organização
```

Observação: os tipos de restrição Criar, Excluir, Pré-atualizar e Atualizar agora oferecem suporte a uniões a outras tabelas. Também podem incluir referências no formulário @root.attribute para atributos no registro de contato para o usuário atual.

Criar uma restrição de partição de dados para atribuições do CAB

Você pode criar uma restrição de partição de dados que permita aos usuários atualizar somente requisições de mudança atribuídas ao CAB a que o usuário conectado pertence.

Para criar uma restrição de partição de dados para atribuições de usuário de requisição de mudança do CAB, atribua os seguintes valores de restrição a uma tabela Change_Request controlada em uma partição de dados:

- Tipo de restrição: Pré-atualizar
- Especificação da restrição: cab.[group]group_list.member IN (@root.id)

O usuário conectado pode atualizar somente requisições de mudança atribuídas a um CAB a que o usuário pertence.

Mais informações:

Console do CAB e geração de relatório (na página 814)

Configure as restrições da partição de dados do Gerenciamento de conhecimento para permissões com base em função

As partições de dados do Gerenciamento de conhecimento são ativadas para permitir o uso de permissões de grupo e função por padrão no CA SDM. Se você estiver atualizando de um release anterior, a ferramenta de migração atualiza as restrições da partição de dados.

Se você usou restrições da partição de dados personalizadas para gerenciar permissões de conhecimento em um release anterior, atualize as restrições manualmente para as tabelas O_INDEXES e SKELETONS. É possível exibir as restrições da partição de dados e aplicar as mudanças, conforme o adequado para o ambiente.

Para atualizar as restrições da partição de dados

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Partições de dados, Restrições de partição de dados.

   A Lista de restrições da partição de dados aparece.

2. Clique em Mostrar filtro.

   O filtro Pesquisar aparece.

3. Insira **Analista do Service Desk** na pesquisa da Partição de dados.
4. Insira **O_INDEXES** na pesquisa de Tabela.
5. Clique em Pesquisar.

   Os resultados da pesquisa são exibidos.

6. Clique no tipo de restrição *Exibição*.

   A página Detalhes da restrição da partição de dados aparece.

7. Clique em Editar.

   A página Atualizar restrição da partição de dados aparece.

8. Modifique a guia Restrição para substituir "READ_PGROUP in @root.pgroups" como segue:

   ```
   READ_PGROUP in @root.pgroups OR
   READ_PGROUP.[pgroup]contained_roles.role IN @root.id
   ```

   Salve a restrição.

9. Abra os tipos de restrição *Exclusão* e *Pré-atualização* a partir da Lista de restrições da partição de dados.

10. Modifique a guia Restrições para substituir "WRITE_PGROUP in @root.pgroups" em *Exclusão* e *Pré-atualização* como segue:

    ```
    WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN
    @root.role
    ```

11. Salve as restrições.

12. Repita as etapas para atualizar as restrições de *Exibição*, *Exclusão* e *Pré-atualização* na tabela *SKELETONS* na sua partição de dados.

    As restrições da partição de dados são atualizadas.

Pesquisas

As pesquisas de cliente permitem aos administradores do CA SDM coletar e analisar sistematicamente os comentários do cliente sobre o desempenho do service dsk. Você pode personalizar pesquisas para que elas atendam às necessidades de sua localidade.

Configurar seu sistema para pesquisas

Para poder utilizar pesquisas, você deverá configurar seu sistema adequadamente, o que envolve duas etapas:

1. Instale e configure a interface da web de CA SDM. Quando um usuário acessa o URL de uma pesquisa, a interface da Web formata e preenche a pesquisa com informações. Consulte o *Guia de Implementação* para obter mais informações.

2. Usando o Gerenciador de opções, configure e instale a opção web_cgi_url para especificar o local do mecanismo da Web do CA SDM. Consulte o capítulo "Controlando o comportamento do sistema" e a *Ajuda online* para obter detalhes.

Preparar uma pesquisa

As pesquisas são preparadas usando a Lista de pesquisas de cliente, que é uma janela típica de lista. Por exemplo, você pode usar essa janela para exibir todas as pesquisas ou um subconjunto filtrado de acordo com um critério de busca digitado; pode criar novas pesquisas; pode exibir detalhes de uma pesquisa particular e pode criar relatórios com as pesquisas na lista.

Cada pesquisa tem as seguintes características que podem ser definidas:

- Um nome que você pode usar ao buscar pesquisas e criar relatórios
- Uma introdução que você pode usar para explicar o propósito da pesquisa aos clientes
- Uma lista classificada de perguntas para o cliente responder, e cada pergunta inclui um conjunto de respostas possíveis
- Uma área opcional em que o usuário pode digitar comentários em formato livre
- Uma mensagem de conclusão a ser exibida depois que o usuário envia a pesquisa de volta

Observação: para obter mais informações sobre como criar pesquisas, consulte a *Ajuda online*.

Definir notificações de pesquisa

A guia Pesquisa na página Atualizar notificação de atividade permite definir uma notificação de pesquisa para uma notificação de atividade. Quando a atividade de notificação é acionada, o contato que iniciou a atividade recebe a notificação de pesquisa. Um log de atividades é gerado quando uma notificação de pesquisa é enviada e quando é recebida de volta de um cliente.

Para configurar uma notificação de pesquisa

1. Na guia Administração, vá para Notificações, Notificações de atividade.

   A Lista de notificações de atividade aparece.

2. Selecione a notificação de atividade desejada.

   A página de detalhes é exibida.

3. Clique no botão Editar.

   A página Atualizar notificação de atividade é exibida.

4. Edite os campos conforme apropriado.
5. Selecione o tipo apropriado de objeto na lista suspensa.

6. Clique na guia Pesquisa.

   Essa guia contém os seguintes campos:

   Enviar pesquisa

   Esta caixa de seleção permite ativar ou desativar a pesquisa. Se selecionada, a pesquisa é enviada ao contato quando a notificação da atividade selecionada for acionada.

   Pesquisa padrão

   Especifique uma pesquisa padrão usando o ícone pesquisar ou especifique sua própria na caixa de texto.

   Método de notificação

   Escolha *um* dos seguintes métodos de notificação:

   - Email
   - Notificação
   - Pager_Email

   Título da mensagem de pesquisa

   Digite o título da pesquisa.

   Corpo da mensagem de pesquisa

   Digite uma mensagem para o contato. Quando um usuário recebe notificação de uma pesquisa, o corpo da mensagem automaticamente inclui um URL que pode ser acessado em um navegador da Web para localizar e preencher o formulário de pesquisa.

7. Salve a notificação da atividade.

   Quando a atividade de notificação é acionada, o contato que iniciou a atividade recebe a notificação de pesquisa.

Criando relatórios da pesquisa

O CA SDM permite criar relatórios de pesquisas usando as guias de administração do Web Client de todos os modos normalmente empregados. Por exemplo, na janela Lista de pesquisas de cliente, você pode escolher Relatórios do menu Arquivo e escolher um relatório de Resumo ou Detalhes. Você também pode escolher Imprimir formulário nas várias janelas de detalhe para imprimir os dados de formulário de suas pesquisas, perguntas e respostas.

Você também pode criar seus próprios relatórios com base nos dados de pesquisa no banco de dados do CA SDM.

Pesquisa gerenciada

A Pesquisa gerenciada permite ao administrador do CA SDM selecionar uma população de pesquisa de amostra desejada e combiná-la a uma pesquisa específica. Em seguida, o administrador pode distribuir solicitações a clientes específicos que deverão responder à pesquisa num momento determinado. Isso proporciona ao administrador a flexibilidade para criar períodos de pesquisa abertos, ao mesmo tempo que mantém a capacidade de usar pesquisas com base em atividade e em categoria relacionadas a Solicitações, Requisições de mudança e Ocorrências.

O propósito das Pesquisas gerenciadas é fornecer um mecanismo para administrar pesquisas. Essa função pode ser útil ao usar formulários de pesquisa que necessitam ser controlados regularmente (por exemplo, pesquisas usadas apenas durante um período curto a cada ano ou pesquisas que estejam offline por muito tempo).

Importante: Se você desejar enviar a pesquisa a um grande número de contatos, defina o valor de NX_SURVEY_ILIMIT in NX.env em um limite superior, como 1073741824.

Observação: para obter mais informações sobre como criar pesquisas, consulte a *Ajuda online*.

Web Services

Os serviços web se adaptam aos padrões de troca de dados, que fazem o seguinte:

- Permitem aos aplicativos se comunicar através de HTTP com vários servidores, independentemente do ambiente operacional.
- Permitem que a maioria dos aplicativos acesse a funcionalidade de produtos CA.
- Permite a clientes dos serviços da web criar tickets, atualizar ativos, pesquisar a base de conhecimento e muito mais.

Observação: para obter mais informações, consulte Gerenciando serviços web no *Guia de Implementação*.

Capítulo 5: Configurando contas de usuário

Esta seção contém os seguintes tópicos:

Contatos (na página 215)
Definições de contato (na página 215)
Grupos (na página 217)
Tipos de contato (na página 218)
Tipos de tratamento especiais (na página 219)
Dados no diretório LDAP (na página 222)

Contatos

Uma parte importante do estabelecimento de um service desk operacional é definir os usuários que a ele terão acesso. No CA SDM, usuários são *contatos* nomeados, e é possível realizar várias tarefas para defini-los e gerenciá-los:

- Configurar manualmente os contatos.
- Organizar contatos em grupos que definem áreas de responsabilidade.
- Estabelecer tipos de contato para organizar seus contatos do CA SDM em grupos lógicos de acordo com o uso que fazem do sistema.
- Importar informações de usuário LDAP em um registro de contato do CA SDM.
- Atribuir um contato a uma função para definir a funcionalidade de sistema acessível.
- Atribuir um tipo de tratamento especial, como Pessoa muito importante (VIP), a um contato.

Definições de contato

Todos que utilizarem o CA SDM deverão ser definidos como contatos. Um registro de contato de usuário define as informações de que o sistema necessidade da seguinte forma:

Identificação básica

Define a identificação básica, como nome do usuário e tipo de contato. O nome do contato é usado como o identificador primário quando você seleciona um contato ou digita informações de contato em outros contextos.

Login

Define informações de logon, como a ID de usuário e, alguns casos, um campo PIN para ser usado como a senha que verifica o usuário durante o logon. A ID de usuário é usada para identificar o usuário na tabela de contatos para fins de autenticação e para determinar os tipos de acesso atribuídos ao usuário. Dependendo de como o administrador configurou a segurança, outro campo, como ID de contato, pode ser usado como o campo PIN e o usuário pode usá-la como a senha de logon.

Segurança

Define o tipo de acesso que é atribuído em seu registro de contato ou com um tipo de acesso padrão, dependendo de como a segurança foi configurada em seu sistema. Além disso, um tipo de acesso do usuário pode ser atribuído de acordo com sua participação em um grupo do Diretório LDAP.

O tipo de acesso de um usuário determina todos os aspectos de sua segurança, incluindo como será autenticado no sistema, que interface web ele verá e que funções do produto ele poderá acessar

O gerenciamento da segurança é um recurso da interface web.

Tipo de serviço

Determina o nível de serviço que um usuário recebe. O tipo de serviço do contato define o nível de serviço do qual o usuário usufrui. Os SLAs são negociados com os clientes do CA SDM, e tipos de serviço servem como o mecanismo usado pelo CA SDM para implementar SLAs. Ao associar um tipo de serviço a um registro de contato do usuário, você pode garantir que, ao criar um ticket no qual um usuário é identificado como o usuário final afetado, o tipo de serviço do ticket estará de acordo com o tipo de serviço definido para o contato.

A configuração de SLAs usando tipos de serviço é um recurso que você, como o administrador, realiza usando a interface web.

Atribuição automática

Define informações de atribuição automática, como turno de trabalho e disponibilidade (usadas apenas para tipos de contato de analista). Você pode configurar contatos de analista para determinar se podem ser usados com a atribuição automática. A atribuição automática é válida apenas para solicitações, e é definida como parte da configuração da área de solicitação. Está também associada aos grupos aos quais o analista pertence.

Como enviar mensagens de notificação aos usuários

Define as informações de notificação de um contato que incluem o seguinte:

- vários endereços de email e números de telefone a ser usado para notificações
- método a ser usado para notificações com diferentes níveis de urgência
- turnos de trabalho durante os quais serão recebidas notificações

O cálculo do atraso da notificação leva em consideração o Fuso horário do contato. Se o fuso horário do contato não for definido, o fuso horário do servidor é usado em seu lugar. Usando o fuso-horário do servidor pode resultar em notificações disparadas às vezes, percebidas fora das configurações do Turno de trabalho.

Informações da organização (como local, organização e departamento) permitem agrupar contatos de acordo com a organização a que pertencem. Por exemplo, associar um contato a um local vincula o contato a um endereço físico e também ajuda a determinar a atribuição automática. Um tipo de serviço pode ser atribuída à organização, tornando mais fácil a administração de contratos de nível de serviço por organização do que por contato individual.

Grupos aos quais um usuário pertence

Organiza contatos em grupos que representam áreas específicas de responsabilidade em sua central de serviços. Você pode configurar e definir contatos usando a interface web.

Grupos

Um grupo é um conjunto de contatos que compartilham uma área de responsabilidade comum. No CA SDM, os grupos são implementados usando o tipo de contato de grupo predefinido, o que torna um grupo somente um tipo de contato especial. Um grupo apresenta as mesmas informações básicas de um contato, com a característica adicional importante de que grupos são essenciais para a atribuição automática de solicitações. Você pode associar áreas de solicitação, locais e um turno a um grupo. Esses atributos são usados para determinar se e quando os contatos no grupo podem aceitar a atribuição automática de uma solicitação.

Observação: para obter informações definição de grupos, consulte a *Ajuda online*.

Tipos de contato

Os tipos de contato são usados para categorizar os usuários do CA SDM em grupos lógicos de acordo com o uso que fazem do sistema. Por exemplo, entre os tipos de contato predefinidos pelo sistema estão analista, cliente e grupo. Estes tipos de contato predefinidos atendem às necessidades da maioria das implementações do CA SDM; no entanto, se suas circunstâncias assim o exigirem, é possível modificar os tipos de contato predefinidos e criar tipos de contato. Quando definir os usuários como contatos, é possível associar um tipo de contato a cada um deles.

Observação: para obter mais informações sobre a definição de tipos de contato, consulte a *Ajuda online*.

Determinar o comportamento de acordo com o tipo de contato

O *tipo* de contato determina que contatos são exibidos (e têm permissão) em situações diferentes. Por exemplo, quando você atribui manualmente qualquer tipo de ticket, como uma solicitação ou uma ocorrência, o campo para especificar o destinatário exige que a pessoa à qual você especifica tenha um tipo de contato de analista. Se você escolher selecionar um contato de uma lista de seleção para esse campo, apenas contatos do tipo analista serão exibidos na lista de seleção. Inserir um contato com um tipo diferente exibirá a tela de pesquisa de somente analistas.

Observação: um recurso importante do tipo de contato é a implementação de grupos de contatos por meio do tipo de contato de grupo predefinido.

Configuração de notificação com base no tipo de contato

Você pode basear a notificação no tipo de contato, o que permite enviar uma mensagem de notificação a todos os contatos de um tipo particular.

Mais informações:

Notificações (na página 101)

Selecionar contatos de acordo com o tipo de contato

Você pode selecionar usuários de acordo com o tipo de contato em vários contextos. Por exemplo, a maioria das janelas de lista e seleção que exibem esses contatos têm um campo de pesquisa onde você pode selecionar um tipo de contato como critérios de pesquisa.

Tipos de tratamento especiais

É possível definir tipos de tratamento especial que identifiquem contatos que requerem atenção especial. É possível usar os tipos de tratamento especial que o CA SDM fornece ou criar seus próprios tipos. É possível visualizar e localizar tickets que especificam um usuário final afetado que requer atenção especial. Por exemplo, analistas podem navegar na pasta VIP pasta no Gerenciador de filas para identificar tickets que especificam um VIP como o usuário final afetado.

Os exemplos a seguir são contatos que tipos especiais de tratamento podem identificar:

- Pessoas Muito Importantes (VIPs), como executivos
- Clientes com renovação de suporte em andamento
- Clientes com deficiências que necessitem de tratamento ou equipamento especial
- Visitantes
- Contatos suspeitos de uso indevido ou abuso dos recursos do sistema

Quando um ou mais tipos de tratamento especial são atribuídos a um contato, os tickets que especificam o contato no campo Usuário final afetado mostram um banner ou ícone de alerta ou ambos. É possível usar campos de tickets e tipos de tratamento especial para acompanhar tickets e distinguir entre dois tipos de contato relacionados, porém possivelmente distintos. Por exemplo, um VIP (Usuário final afetado) possui um assistente (Solicitante) atuando em seu nome. Quando o Usuário final afetado é um contato atribuído a um tipo de tratamento especial VIP, um analista pode priorizar tickets com mais precisão.

Mais informações:

Como configurar contatos de tratamento especial (na página 220)
Associar um contato a um tipo de tratamento especial (na página 221)

Como configurar contatos de tratamento especial

Para configurar contatos de tratamento especial, siga as seguintes etapas:

1. Crie tipos de tratamento especial.
2. Associe um contato a qualquer número de tipos de tratamento especial (na página 221). Similarmente, um tipo de tratamento especial pode ter muitos contatos.

   Um contato associado a um ou mais tipos de Tratamento especial é visualmente distinguido no formulário de Detalhes do contato e o navegador de Perfil rápido usando uma faixa no alto de cada página. Essa faixa exibe um ícone de alerta e um texto de alerta para cada tipo de Tratamento especial atribuído ao contato.

   Além disso, quaisquer tickets que identificam o contato como o Usuário final afetado são indicados como segue:

   - Ícones de Alerta e texto de Alerta aparecem em uma faixa na parte superior do formulário de detalhes do ticket.
   - Ícones de Alerta aparecem na lista de ticket.
   - O Gerenciador de filas inclui uma pasta e subpastas V.I.P. para cada tipo de ticket. V.I.P. subpastas incluem tickets para usuários finais afetados que são contatos de tratamento especial VIP.

     Observação: a pasta Gerenciador de filas V.I.P. é exibida para funções de analista.

Mais informações

Associar um contato a um tipo de tratamento especial (na página 221)

Associar um contato a um tipo de tratamento especial

É possível atribuir um tipo de tratamento especial a um contato para alertar os analistas sobre tickets que afetam usuários finais com requisitos especiais, como para pessoa com deficiência visual, um contato que representa um risco de segurança, e assim por diante.

Para associar um contato a um tipo de tratamento especial.

1. Na página Detalhes do contato, selecione a guia Tratamento especial.

   A guia Lista de tratamentos especiais associados relaciona os tipos de tratamento especial que estão associados ao contato.

2. Clique no botão Atualizar tratamentos especiais do contato.

   O filtro Pesquisar aparece.

3. Pesquisar o tipo de tratamento especial que deseja associar ao contato.

   A página Atualização de tratamentos especiais é exibida.

4. Selecione um ou mais tipos de tratamento especial na coluna à esquerda e use o botão mover (>>) para mover os tipos para a coluna da direita. Clique em OK.

   Observação: você pode remover uma associação de um contato usando o botão mover (<<) para mover o tipo da coluna da direita para a coluna da esquerda. Você pode clicar no ícone de pesquisa para pesquisar o valor desejado.

   O contato está associado a um tipo de tratamento.

   O CA SDM exibe quaisquer dos seguintes, dependendo do tipo de tratamento, quando um ticket especifica o contato no campo Usuário final afetado:

   - Uma faixa de alerta aparece em Detalhes do contato para o usuário final afetado em um ticket.
   - O texto de alerta é exibido como uma faixa no alto da página de detalhes do ticket e no Perfil resumido.
   - Listas de ticket destacam a linha de contato e mostram um sinalizador de alerta.
   - Uma pasta V.I.P. é exibida no Gerenciador de filas para funções de analista. A pasta contém todos os tickets associados aos contatos (Usuários finais afetados) que possuem um tipo de tratamento especial VIP.

Dados no diretório LDAP

O *LDAP* (Lightweight Directory Access Protocol) é um protocolo de comunicação de rede para consulta e modificação de serviços de diretório executando em uma rede TCP/IP. Um diretório LDAP é uma estrutura em árvore que contém entradas para gerenciamento de usuários, grupos, computadores, impressoras e outras entidades em uma rede.

O CA SDM pode ser configurado para acessar um diretório LDAP, que permite usar os dados LDAP de várias maneiras:

- Sincronizar contatos com registros de usuário LDAP. A sincronização pode ocorrer das seguintes formas:
  - **No logon**—Quando um usuário efetua o logon no produto, se existir um registro LDAP para aquele usuário, mas o registro de contato correspondente não existir, um registro de contato é automaticamente criado com base nas informações do LDAP.
  - **Novo Contato**—Quando você cria um contato manualmente, pode selecionar um registro LDAP e mesclar seus valores de atributo com seus campos correspondentes no novo registro de contato.
  - **Atualização em lote**—É possível executar rotinas em lote para automatizar os processos de importação e atualização de registros de contato com informações dos registros LDAP correspondentes.

    Observação: a sincronização com o LDAP é um processo unilateral. Os dados LDAP podem ser usados para criar e atualizar contatos, mas o produto não oferece suporte às atualizações para o diretório LDAP.
- Atribuir tipos de acesso do CA SDM com base na inscrição em grupos do LDAP.
- Implementar um método alternativo de realizar a autenticação no CA SDM.

Observação: o componente ldap_virtb fornece funcionalidade de integração com LDAP; é instalado com o CA SDM por padrão e pode ser executado em um servidor primário ou secundário, independentemente do tipo de sistema operacional. Para obter informações, consulte o *Guia de Implementação*. O arquivo $NX_ROOT/bopcfg/majic/ldap.maj especifica o mapeamento entre atributos LDAP e atributos de registro de contato.

Importante: O CA SDM requer que registros LDAP tenham uma entrada no campo sobrenome para pesquisar, exibir e importar os dados LDAP.

Importante: O CA SDM oferece suporte a *pesquisa paginada*, que pesquisa todos os registros em seu diretório LDAP. A pesquisa paginada também permite importar novos registros de contato ou sincronizar registros de contato existentes de qualquer número de registros LDAP. Esses recursos serão limitados, no entanto, se você estiver usando o Sun Java System Directory Server ou o Novell eDirectory, pois esses servidores LDAP não oferecem suporte a pesquisa paginada. Neste caso, é possível somente pesquisar, importar e sincronizar com o número de registros LDAP especificados por NX_LDAP_MAX_FETCH. Para obter mais informações, consulte o arquivo NX.env (na página 239).

Configurar opções de LDAP

Você pode configurar o CA SDM para acessar dados do diretório LDAP.

Para configurar o CA SDM para acessar dados do diretório LDAP

1. Instale manualmente as opções do LDAP usando o Gerenciador de opções da interface da web.

   Observação: as opções necessárias para integração básica com LDAP são identificadas como obrigatórias na coluna Descrição na tabela a seguir. As opções identificadas como opcionais são recursos que só poderão ser adicionados se todas as opções obrigatórias estiverem instaladas. Os valores que você especifica ao instalar estas opções são gravados no arquivo $NX_ROOT/NX.env. Para obter mais informações sobre as opções de LDAP e instruções para instalá-las, consulte a *Ajuda online.*

2. Reinicie o serviço do CA SDM.

   As mudanças entram em vigor.

Opção	Valor padrão	Descrição
default_ldap_tenant		Exigido para instalação de multilocação. Especifica a atribuição de inquilino padrão para contatos importados do LDAP. Você deve usar o inquilino UUID ao configurar o campo Valor da opção. **Observação:** você pode obter a UUID do inquilino em uma consulta ao banco de dados. Por exemplo, "SELECT * FROM ca_tenant".
ldap_enable	Sim	Obrigatório. Ativa a integração do LDAP com o CA SDM.
ldap_host		Obrigatório. Especifica o endereço IP ou o nome de host do servidor de banco de dados LDAP.
ldap_port	389	Obrigatório. Especifica o número da porta do servidor LDAP.
ldap_dn		Obrigatório. Especifica o distinguishedName de logon de servidor LDAP. **Por exemplo**: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com Se o servidor LDAP aceitar vínculos anônimos, este valor pode estar vazio.
ldap_pwd		Obrigatório. Especifica a senha para o distinguishedName de logon de servidor LDAP. Se o servidor LDAP aceitar vínculos anônimos, este valor pode estar vazio.
ldap_search_base		Obrigatório. Especifica o ponto inicial para pesquisas na árvore de esquema de LDAP: (UNIX) Você deve especificar um contêiner inicial. Por exemplo: CN=Users, DC=KLAND, DC=AD, DC=com (Windows) Você não precisa especificar um contêiner. Você pode iniciar no alto da árvore do esquema. Por exemplo: DC=KLAND, DC=AD, DC=com

Opção	Valor padrão	Descrição
ldap_filter_prefix	(&(objectClass= user)	Especifica o prefixo aplicado a um filtro gerado automaticamente durante a pesquisa por usuários LDAP. **Observação:** Esta variável foi substituída pela opção ldap_user_object_class. Não está disponível no Gerenciador de opções, mas pode ser configurado manualmente no arquivo NX.env.
ldap_filter_suffix	)	Especifica o sufixo aplicado a um filtro automaticamente gerado durante pesquisa por usuários LDAP. **Observação:** Esta variável foi substituída pela opção ldap_user_object_class. Não está disponível no Gerenciador de opções, mas pode ser configurado manualmente no arquivo NX.env.
ldap_user_object_ class	pessoa	Obrigatório. Especifica o valor do atributo objectClass do LDAP aplicado a um filtro gerado automaticamente ao pesquisar para usuários LDAP.
ldap_enable_group	Sim	Opcional Ativa a atribuição do tipo de acesso do CA SDM com base na inscrição do grupo LDAP.
ldap_group_object_ class	group	Obrigatório somente se ldap_enable_group estiver instalado. Especifica o nome de objeto aplicado a um filtro gerado automaticamente durante a pesquisa por grupos.
ldap_group_filter_ prefixo	(&(objectClass= group)	Especifica o prefixo aplicado a um filtro gerado automaticamente ao pesquisar por grupos LDAP. **Observação:** Esta variável foi substituída pela opção ldap_group_object_class. Não está disponível no Gerenciador de opções, mas pode ser configurado manualmente no arquivo NX.env.
ldap_group_filter_ sufixo	)	Especifica o sufixo aplicado a um filtro gerado automaticamente ao pesquisar por grupos LDAP. **Observação:** Esta variável foi substituída pela opção ldap_group_object_class. Não está disponível no Gerenciador de opções, mas pode ser configurado manualmente no arquivo NX.env.
ldap_enable_auto	Sim	Opcional Ativa a geração automática de registros de contato dos dados LDAP.

Opção	Valor padrão	Descrição
ldap_sync_on_null	Sim	Opcional Substitui atributos de contato do CA SDM existentes por dados nulos se o atributo de usuário LDAP correspondente contiver um valor nulo.
ldap_service_type	Active Directory	Opcional Use essa opção se o ambiente operacional do CA SDM no Windows e no diretório LDAP *não* for Active Directory (por exemplo, se for eTrust ou Novell). **Observação:** em ambientes operacionais UNIX, a funcionalidade "Não-AD" só é usada se essa opção *não* estiver instalada. Se estiver instalado, o tipo de serviço é definido como Diretório ativo.
ldap_enable_tls	Não	Opcional Especifica se TLS (Transport Layer Security) está habilitado durante o processamento de LDAP.

Verifique a integração LDAP

Após a instalação das opções de LDAP necessárias, os usuários do CA SDM podem importar dados LDAP caso a caso, sem necessidade de preencher todos os campos de atributo de contato manualmente.

Para verificar se a integração com LDAP está corretamente configurada, execute as seguintes etapas usando a interface da web. Se encontrar problemas, consulte Solução de problemas (na página 238).

Para verificar se você pode pesquisar e importar registros LDAP.

1. Selecione Arquivo, Novo contato do LDAP na guia Service Desk.

   A janela Pesquisa de diretório LDAP é exibida.

2. Especifique os critérios de filtro e, então, clique em Pesquisar. Por exemplo, você pode digitar b% no campo Sobrenome para recuperar uma lista das entradas de usuário LDAP com os sobrenomes que começam com a letra B.

   Observação: Se seu diretório LDAP contém milhares de entradas e você não filtrar sua pesquisa, sua solicitação tenta recuperar *todos* os registros de usuário LDAP. Isso pode fazer a solicitação alcançar o tempo limite e retornar zero registro.

   São exibidos os resultados da pesquisa que corresponderem a seus critérios de filtro.

3. Selecione uma entrada.

   A janela Criar novo contato é exibida, preenchida com valores de atributo importados do LDAP.

4. Clique em Salvar.

   O registro de contato é criado.

Para verificar se você pode atualizar um contato usando os dados LDAP

Observação: antes de realizar esse procedimento, para fins de teste, você pode querer usar qualquer ferramenta de edição LDAP que tenha disponível para alterar um ou mais valores de atributo na entrada usada para o procedimento anterior. Você pode verificar se o contato está atualizado com os últimos dados LDAP.

1. Selecione Pesquisar, Contatos na guia Service Desk.

   A janela Pesquisa de contato é exibida.

2. Especifique os critérios de filtro para um contato que possui uma entrada de usuário LDAP correspondente. Por exemplo, é possível pesquisar o contato criado no procedimento anterior.

   São exibidos os resultados da pesquisa que corresponderem a seus critérios de filtro.

3. Selecione o contato que deseja atualizar com os dados LDAP.

   A página Detalhes do contato é exibida, preenchida com as informações de contato do CA SDM.

4. Clique em Editar.

   A página Atualização de contatos aparece.

5. Clique em Mesclar LDAP.

   A página Lista de entrada LDAP exibe uma lista de entradas de usuário LDAP que correspondem ao contato selecionado do CA SDM.

   Para pesquisar no diretório LDAP por outras entradas, você pode clicar em Exibir filtro, especificar os critérios de filtro e clicar em Pesquisar.

   Observação: Se seu diretório LDAP contém milhares de entradas e você não filtrar sua pesquisa, sua solicitação tenta recuperar *todos* os registros de usuário LDAP. Isso pode fazer a solicitação alcançar o tempo limite e retornar zero registro.

6. Clique na entrada LDAP de interesse.

   A página Detalhes do LDAP exibe os valores de atributo para a entrada selecionada. Verifique se você selecionou a entrada correta para o contato que deseja atualizar, então clique em Fechar janela.

7. Na página Lista de entrada LDAP, Clique com o botão direito do mouse na entrada que melhor corresponde ao contato que você deseja atualizar e então selecione Mesclar no contato.

   A página Atualização de contato é exibida novamente, preenchida com os valores de atributo LDAP atuais. Se os dados LDAP foram alterados desde que você criou ou atualizou o contato, as mudanças são refletidas nos campos de atributo do contato.

   Observação: se você tem a opção ldap_sync_on_null instalada e a entrada LDAP contém valores nulos para quaisquer campos de atributo que correspondem aos atributos de contato que atualmente contêm valores, os valores no registro de contato são substituídos por valores nulos quando você salva os dados do contato.

8. Clique em Salvar na página Atualizar contato.

   O contato é atualizado com os dados LDAP correspondentes.

Criar um contato automaticamente

É possível configurar o CA SDM para criar um contato automaticamente a partir de um registro de usuário LDAP correspondente sempre que um novo usuário efetuar logon no CA SDM.

Para ativar esse recurso, instale todas as opções de LDAP obrigatórias mais a opção ldap_enable_auto.

O registro de contato é criado automaticamente, como segue:

1. Se um usuário que efetuou logon no CA SDM ainda não possuir um registro de contato, mas o seu nome de logon existir em um registro LDAP, os dados LDAP são automaticamente importados e o registro de contato é criado.
2. O registro de contato criado automaticamente herda as configurações de segurança de tipo de acesso padrão.
3. Então pode ser atribuído explicitamente um tipo de acesso ao contato, ou o tipo de acesso pode ser atribuído com base na inscrição do usuário em um Grupo LDAP.

Esse processo é completamente transparente para o usuário, aparecendo como qualquer outra sessão de logon.

Atribuições de tipo de acesso a partir de grupos LDAP

É possível configurar o CA SDM para atribuir valores de tipo de acesso a contatos automaticamente, com base na inscrição em grupos LDAP. Com a atribuição automática de tipo de acesso habilitada, se um registro de usuário LDAP que tiver sido usado para criar um contato pertencer a um grupo LDAP associado com um dos tipos de acesso do CA SDM, então o tipo de acesso é automaticamente atribuído ao contato. Caso contrário, o contato herdará o tipo de acesso padrão.

Para ativar a atribuição automática de tipo de acesso, é preciso instalar as opções ldap_enable_group e ldap_group_object_class.

Observação: para obter detalhes sobre a instalação das opções necessárias e associação de grupos LDAP com tipos de acesso, consulte a *Ajuda online*.

Importação em lote de contatos usando dados LDAP

É possível executar o utilitário de linha de comando pdm_ldap_import para criar contatos do CA SDM no modo de lote usando dados LDAP.

Observação: além de criar contatos, o pdm_ldap_import atualiza contatos existentes se não estiverem sincronizados com suas entradas LDAP correspondentes. É possível usar o processo de lote pdm_ldap_sync para atualizar contatos existentes, mas não para criar novos contatos.

O pdm_ldap_import possui a seguinte sintaxe:

```
pdm_ldap_import -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "*ldap_where_clause*"

Especifica as ids de usuário de registros LDAP a serem pesquisados. As variáveis de substituição são indicadas com o caracteres '?'. Por exemplo, para *userid = ?*. O valor padrão é *userid = ?*. Nesse caso especial, a id é mapeada para ao atributo de contato ldap_dn.

Observação: use as palavras-chave, conforme definidas no arquivo *ldap.maj*. Você também pode pesquisar usando a sintaxe memberOf = 'group_dn'.

-c "*contact_where_clause*"

(Opcional) Especifica como determinar se o registro do contato já existe. Se o registro do contato não existir, um novo registro do contato é inserido. Se o registro do contato existir e não estiver sincronizado com os dados LDAP atuais, o registro do contato é atualizado.

-u "*userid*"

(Opcional) Especifica o nome de logon sob o qual o programa pdm_ldap_import é executado.

Observação: é possível usar curingas com o pdm_ldap_import para especificar vários registros.

Exemplos: importações em lote usando dados LDAP

Este exemplo importa um único registro LDAP para a id de usuário jsmith11:

```
pdm_ldap_import -l "userid = 'jsmith11'"
```

Este exemplo importa todos os registros LDAP com uma id de usuário que inicie com a letra C:

```
pdm_ldap_import -l "userid = 'c%'"
```

Este exemplo importa todos os registros de usuários LDAP no diretório:

```
pdm_ldap_import -l "userid = '%'"
```

Mais informações:

Atualização em lote de contatos usando dados LDAP (na página 233)

Importação de contatos em lote por data e hora

É possível configurar o utilitário pdm_ldap_import para importar registros LDAP que foram criados antes ou depois de uma data e hora específicas. Para ativar esta funcionalidade, crie um arquivo ldap.mod com o seguinte conteúdo:

```
OBJECT ldap {
  ATTRIBUTES LDAP_Entry {
    whenCreated whenCreated STRING ;
  };
};
```

Isto adiciona o atributo *whenCreated* ao objeto LDAP.

As regras para filtrar registros usando o atributo whenCreated são as seguintes:

- Use somente o operador >= ou <=.
- Especifique *todos* os caracteres para o valor data/hora, incluindo o Z. Coloque um 0 em qualquer lugar que não queira explicitamente declarar (por exemplo, a hora do dia).
- Coloque a especificação de data/hora no início do filtro, não use zeros à esquerda no início da sequência de caracteres.
- Não inclua o século à esquerda. Por exemplo, para especificar o ano 2008, use 08.

Observação: aspas simples devem envolver o valor de data/hora.

Exemplo: usando o atributo whenCreated para importar entradas LDAP

O exemplo seguinte usa o atributo whenCreated para importar entradas LDAP criadas depois de 11/3/2008.

```
Pdm_ldap_import -l "whenCreated >= '080312000000Z'"
```

Exemplo: usando o atributo whenCreated para pesquisar registros LDAP

O exemplo seguinte usa o atributo whenCreated com o pdm_ldap_test para pesquisar registros LDAP criados depois de 11/3/2008.

```
pdm_ldap_test.exe -f "whenCreated>=080312000000Z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type : active directory
Service Desk Platform       : windows
Search Base : DC=kirklandsd,DC=ca,DC=com
Search Filter       : (&(objectClass=person)(whenCreated>=080312000000Z))
Administrator Username      :
CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password      : **********
LDAP Host   : gecko.kirklandsd.ca.com
LDAP Port   : 389
LDAP API Version    : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035327.0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035425.0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035726.0Z
3 Total LDAP records found...
```

Resumo e dados de log de importação em lote

O comando pdm_ldap_import mantém um registro detalhado de todas as atividades para cada execução. O arquivo de log ldap_logging.0-n está localizado no diretório $NX_ROOT/log.

O exemplo abaixo mostra os dados de resumo que o pdm_ldap_import retorna na linha de comando:

```
pdm_ldap_import Starting…
pdm_ldap_import Summary:  Processed(21) Updated(1) No Matches(7) New Contacts(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_import Complete…
```

A tabela a seguir descreve os dados de resumo:

Status	Contagem	Descrição
Processed	21	O número total de entradas de LDAP encontradas

Status	Contagem	Descrição
Atualizado	1	O número de registros de contato que foram atualizados por causa da entrada LDAP correspondente contém diferentes informações
No Matches	7	O número de entradas LDAP sem registro de contato correspondente
Novos contatos	11	O número de novos registros de contato que foram criados com base nas entradas LDAP correspondentes
Multiple Matches	0	O número de entradas LDAP com vários registros de contato correspondentes, como definido pela opção ldap_search_base
Empty Filter	2	O número total de entradas de LDAP que não podem ser usadas para gerar um filtro de pesquisa válido
Erros	0	O número de entradas LDAP que encontraram um erro durante o processamento Por exemplo, registros LDAP que não contêm um valor em um campo obrigatório no CA SDM (como Sobrenome) são contados como falhas e não podem ser importados.

Atualização em lote de contatos usando dados LDAP

É possível executar o utilitário pdm_ldap_sync para atualizar registros de contatos em modo de lote usando dados LDAP.

Importante: Este utilitário substitui o inquilino existente do contato LDAP definido no CA SDM. Se desejar reter o valor de inquilino, modifique NX.env, adicionando a variável NX_RETAIN_TENANT_VALUE manualmente e definindo-a para "sim". Se esta variável for definida como "não", ausente, ou não for ajustada adequadamente, o utilitário sobrescreverá as informações do inquilino.

Observação: o utilitário pdm_ldap_sync sincroniza contatos existentes com entradas LDAP correspondentes, mas não cria contatos. É possível usar o processo em lote pdm_ldap_import para criar contatos.

O pdm_ldap_sync possui a seguinte sintaxe:

`pdm_ldap_sync -l "`*`ldap_where_clause`*`" [-c "`*`contact_where_clause`*`"] [-u "`*`userid`*`"]`

-l "ldap_where_clause"

Determina como pesquisar por registros LDAP correspondentes. As variáveis de substituição são indicadas com o caracteres '?'. Por exemplo, para *id_do_usuário=?*, o valor padrão é *id =?*. Nesse caso especial, id é mapeada ao ldap_dn do atributo de contato.

-c "contact_where_clause"

(Opcional) Determina quais contatos são usados ao pesquisar por registros LDAP correspondentes.

Padrão: "ldap_dn IS NOT NULL"

-u "userid"

(Opcional) Especifica a id de usuário com a qual o pdm_ldap_sync é executado.

Observação: é possível usar curingas com o pdm_ldap_sync para especificar vários registros.

Exemplos:

Este exemplo estabelece uma linha de base de registros de contato que tenham um registro LDAP correspondente:

```
pdm_ldap_sync -l "userid = ?" -c ""
```

Este exemplo usa os parâmetros padrão para atualizar todos os contatos que tenham um distinguishedName do LDAP:

```
pdm_ldap_sync
```

Este exemplo atualiza um único contato:

```
pdm_ldap_sync -l "userid = ?" -c "userid = 'jsmith11'"
```

Mais informações:

Importação em lote de contatos usando dados LDAP (na página 230)

Resumo e dados de log de atualização em lote

O comando pdm_ldap_sync mantém um registro detalhado de todas as atividades para cada execução. O arquivo ldap_logging.0-n está localizado no diretório $NX_ROOT/log.

O exemplo abaixo é um exemplo de dados de resumo que o pdm_ldap_sync retorna na linha de comando:

```
pdm_ldap_sync Starting…
pdm_ldap_sync Summary:  Processed(21) Updated(1) No Matches(7) No Changes(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_sync Complete…
```

A tabela a seguir descreve os dados de resumo:

Status	Contagem	Descrição
Processed	21	O número total de entradas de LDAP encontradas
Atualizado	1	O número de entradas LDAP com informações diferentes de seus registros de contato correspondentes no CA SDM
No Matches	7	O número de entradas LDAP sem registro de contato correspondente no CA SDM
No Changes	11	O número de entradas LDAP com informações idênticas às de seus registros de contato correspondentes no CA SDM
Multiple Matches	0	O número de entradas LDAP com vários registros de contato correspondentes no CA SDM, como definido pela opção ldap_search_base
Empty Filter	2	O número total de entradas de LDAP que não podem ser usadas para gerar um filtro de pesquisa válido
Erros	0	O número de entradas LDAP que encontraram um erro durante o processamento

Autenticação LDAP

Você pode usar o LDAP para autenticar usuários que façam logon no CA SDM. A autenticação LDAP está disponível quando o componente de autenticação do CA EEM está integrado com o CA SDM, que substitui a validação padrão realizada pelo sistema operacional host. A autenticação LDAP é aplicável apenas quando o CA EEM está configurado para usar um diretório LDAP externo e você selecionou autenticação de SO para um tipo de validação do usuário em um registro de tipo de acesso.

Quando um recurso do CA EEM é ativado, as solicitações de logon são verificadas no servidor do CA EEM. Uma solicitação de logon é concedida somente se ocorrer o seguinte:

- A ID de usuário especificada corresponde a um registro de contato no CA SDM.
- A ID do usuário corresponde a um perfil de usuário no CA EEM.
- A combinação da ID do usuário com a senha é validada com êxito pelo CA EEM.

Observação: para obter mais informações sobre o uso da autenticação do CA EEM, consulte o *Guia de Implementação*. Para obter mais informações sobre configuração de tipo de acesso, consulte a *Ajuda online*.

Transport Layer Security

É possível configurar o CA SDM para usar TLS (Transport Layer Security) durante o processamento LDAP. O TLS, um protocolo de comunicação seguro, é o sucessor da segurança SSL v3 (Secure Socket Layer). Você instala a opção ldap_enable_tls para ativar o TLS.

Importante: Se este recurso estiver ativado, todas as comunicações entre o CA SDM e o servidor LDAP são criptografadas. Se este recurso *não* estiver ativado, todas as comunicações de dados (incluindo o logon e senha administrativos usados para acessar o servidor LDAP) são enviadas em texto sem formatação.

Observação: para obter informações sobre a configuração do TLS, consulte a documentação de seu servidor LDAP e sistema operacional. Para obter mais informações sobre o uso da opção ldap_enable_tls, consulte a *Ajuda online*.

Mapeamento de atributo

Os valores de atributo de registro de contato do CA SDM são sincronizados com os valores de atributo de usuário do LDAP com base nas definições de mapeamento de atributo no arquivo $NX_ROOT/bopcfg/majic/ldap.maj.

O seguinte trecho do ldap.maj ilustra o mapeamento. Os nomes do atributo na coluna da esquerda (id) são nomes do atributo de contato do CA SDM. A coluna central (distinguishedName) contém os nomes de atributo LDAP correspondentes.

```
    id                distinguishedName               STRING 512;
last_name          sn,pzLastName                     STRING ;
first_name         givenName,pzFirstName             STRING ;
middle_name     initials,pzMiddleName             STRING ;
userid               uid,sAMAccountName,pzUserName     STRING ;
phone_number    telephoneNumber,pzWorkPhoneNumber STRING ;
```

Se houver um SREL (um relacionamento único ou uma chave estrangeira em outra tabela do banco de dados) no CA SDM, o valor do atributo de contato será sincronizado com o valor LDAP correspondente. Se não houver um SREL, ele não será criado automaticamente durante o processamento da sincronização LDAP.

Observação: por padrão, o mapeamento de atributos é configurado para o esquema LDAP do Microsoft Active Directory. Se necessário, é possível modificar o mapeamento usando um arquivo mod.

Como modificar o mapeamento do atributo

Você pode alterar o mapeamento do atributo padrão.

Para alterar o mapeamento do atributo padrão, execute as seguintes etapas:

1. Navegue até $NX_ROOT/site/mods/majic e abra o arquivo mod.
2. Use instruções MODIFY no arquivo mod como segue.
   - As instruções MODIFY sempre devem ser expressas primeiro no arquivo.
   - Seguindo as instruções MODIFY, todos os campos adicionais que não estiverem no arquivo ldap.maj devem ser declarados com a sintaxe do seguinte exemplo.

- Se você definir um campo que contém um caractere hífen no nome do atributo, é necessário colocar o nome entre aspas simples; caso contrário, ao criar o arquivo mod, o atributo irá falhar com um erro de sintaxe. Por exemplo, o seguinte nome de atributo deve ser colocado entre aspas simples:

  ```
  c_nx_string1 'swsd-secret-question' STRING ;
  ```

3. Salve e feche a arquivo mod.
4. Reinicie o serviço do CA SDM.

   Importante: O mecanismo da web não iniciará se houver uma discrepância na sintaxe ou se letras maiúsculas/minúsculas não coincidirem.

   Suas mudanças têm efeito.

Exemplo: usar instruções MODIFY

O exemplo a seguir mostra como modificar dois campos existentes e adicionar um novo campo.

```
//
// Map CA SDM userid attribute to ADAM Userid
//
MODIFY ldap userid cn ;
MODIFY ldap middle_name middleName ;
OBJECT ldap LDAP {
ATTRIBUTES LDAP_Entry{
contact_num employeeNumber STRING ;
};
} ;
```

Solução de problemas

A principal consideração ao solucionar problemas com um servidor LDAP é que raramente existem duas implementações do LDAP idênticas. Os utilitários do CA SDM podem verificar se a integração com LDAP está funcionando corretamente.

Observação: o CA SDM é pré-configurado para integração somente com o Microsoft Active Directory, eTrust e iPlanet. A integração com outros servidores LDAP geralmente exige mudanças e concessões de ambos os lados.

Mostrar status de daemons ou processos

O processo ldap_virtdb gerencia interações entre o banco de dados virtual do LDAP e o CA SDM.

Para mostrar o status de todos os processos ou daemons CA SDM (UNIX)

1. Execute pdm_status na linha de comando sem nenhum parâmetro:

   ```
   pdm_status
   ```

   O comando pdm_status mostra o status de todos os daemons do CA SDM (UNIX) ou processos (Windows) no sistema a partir do qual o comando é executado, por exemplo:

   ```
   DAEMON                          STATUS      HOST      PID   SLUMP CONNECT TIME
   -----------------------------------------------------------------------------
   --
   Agent antfarm                  Running     antfarm   455   Tue Feb 17 17:55:12
   Ddict_rd             (ddictrd) Completed   antfarm
   Data Dictionary   (ddictbuild) Completed   antfarm
   ...
   User Validation      (boplgin) Running     antfarm   456   Tue Feb 17 17:55:21
   ```

2. Examinar a saída de comando para o status do processo ldap_virtdb.

Comando slstat

Executa o seguinte comando sem parâmetros para verificar se bopLDAP está conectado:

```
slstat
```

Examina a saída do comando para verificar o status do bopLDAP.

Arquivo NX.env

Revise o arquivo $NX_ROOT/NX.env para verificar se as opções de LDAP básicas foram instaladas corretamente.

Dependendo das opções de LDAP instaladas, o arquivo NX.env deverá incluir linhas semelhantes às seguintes:

```
@NX_LDAP_DN=qauser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PWD=OBUNQXo7CmgbThZlCiMKIwJlA3UXdVNAOjUpHjstfDt2LBIDPgwtWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

Importante: Como os servidores Sun Java System Directory Server e Novell eDirectory não oferecem suporte à pesquisa paginada, a pesquisa, importação e sincronização do LDAP são limitadas ao valor dos registros NX_LDAP_MAX_FETCH por invocação. O valor padrão é 100. Se você estiver usando um desses servidores LDAP, adicione NX_LDAP_MAX_FETCH a seu arquivo NX.env para especificar o número máximo de registros LDAP. É possível definir NX_LDAP_MAX_FETCH para qualquer valor menor do que o valor de LDAP_SIZELIMIT_EXCEEDED ou LDAP_ADMINLIMIT_EXCEEDED em seu servidor LDAP.

Mais informações:

Configurar opções de LDAP (na página 223)

pdm_ldap_test

Use o utilitário de linha de comando pdm_ldap_test para testar a conexão com um diretório LDAP, garantir que as opções de pesquisa estão corretamente configuradas e testar a configuração de TLS.

Por padrão, o pdm_ldap_test usa as configurações de parâmetro que são inseridas no arquivo quando você instala, edita ou desinstala as opções de LDAP. Para substituir os padrões, é possível especificar os parâmetros na linha de comando do pdm_ldap_test.

Para ver os parâmetros disponíveis para este comando, insira o seguinte comando:

```
pdm_ldap_test -h
```

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

Verificar conexão ao servidor LDAP

Para verificar a conexão com o servidor LDAP, execute pdm_ldap_test sem parâmetros:

```
pdm_ldap_test
```

Conexão bem-sucedida ao servidor LDAP

Se a conexão for bem sucedida, você receberá uma saída similar à seguinte:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(Administrator) (Success)
LDAP API Versão 3
```

Falha na conexão: servidor inativo, ou nome ou porta incorreta

Se a conexão falhar porque o servidor está inativo ou um nome de servidor LDAP ou porta incorreta foi definido, você receberá uma saída semelhante à seguinte:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

Falha na conexão: LDAP_DN ou LDAP_PWD inválido

Se a conexão falhar porque o LDAP_DN ou LDAP_PWD incorreto foi definido, você receberá saída semelhante à seguinte:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```

Exibir parâmetros de pesquisa

Para verificar se os parâmetros de pesquisa estão corretamente configurados, execute o pdm_ldap_test sem parâmetros:

```
pdm_ldap_test
```

Pesquisa bem-sucedida

Se sua pesquisa for bem-sucedida, você obterá um resultado semelhante à seguinte:

```
DN: CN=John A. Smith,CN=Users,DC=COMPUTERTEST
        c(2)(0): US
        displayName(14)(0): John A. Smith
        mail(14)(0): account02@mycompany.com
        givenName(4)(0): John
        initials(1)(0): a
        distinguishedName(38)(0): CN=John a.
```

```
Smith,CN=Users,DC=COMPUTERTEST
        objectGUID(3)(0): 314738
        pager(12)(0): ###-111-1111
        postalCode(5)(0): 11111
        SAMAccountName(7)(0): account02
        sn(6)(0): Smith
        telephoneNumber(12)(0): ###-342-6265
        userPrincipalName(16)(0): account02@COMPUTERTEST

DN: CN=Mike Johnson,CN=Users,DC=COMPUTERTEST
        displayName(10)(0): Mike Johnson
        givenName(4)(0): Mike
        distinguishedName(34)(0): CN=Mike

Johnson,CN=Users,DC=COMPUTERTEST
        objectGUID(12)(0): 312328
        SAMAccountName(7)(0): account03
        sn(5)(0): Johnson
        userPrincipalName(16)(0): account03@COMPUTERTEST
```

Falha na pesquisa: SEARCH_BASE inválido

Se a pesquisa falhar por causa de um SEARCH_BASE inválido, você receberá saída semelhante à seguinte:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)

ldap_bind_s() (Success)
LDAP API Versão 3
ldap_search_st() (No Such Object or Referral)
```

Falha na pesquisa: SIZELIMIT_EXCEEDED, TIMEOUT

A pesquisa pode não ter êxito e apresentar uma mensagem SIZELIMIT_EXCEEDED ou TIMEOUT se você especificar um filtro que não refine a pesquisa suficientemente. A maioria de servidores LDAP limita o tamanho do conjunto de resultados retornado de uma solicitação de pesquisa. Se você ultrapassar esse limite, receberá uma mensagem SIZELIMIT_EXCEEDED. Se sua solicitação de pesquisa demorar mais do que o tempo limite padrão de 20 segundos, o servidor LDAP interromperá a solicitação e você receberá uma mensagem de erro de TIMEOUT semelhante à seguinte:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Versão 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)
```

Falha na pesquisa: 0 registros retornados

A pesquisa pode não ter êxito porque seu filtro padrão não é correto. Se pdm_ldap_test retornar zero (0) registro, sempre verifique a linha de Usando filtro, que é o filtro base gerado pelo LDAP_FILTER_PREFIX e LDAP_FILTER_SUFFIX, ou as opções de LDAP_OBJECT_CLASS:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabs
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Versão 3
ldap_search_st() 0 records
```

Refinar sua pesquisa

Use o parâmetro -f com o comando pdm_ldap_test para especificar um filtro a ser adicionado ao filtro base para refinar os critérios de pesquisa. Você deve usar sintaxe de LDAP apropriada e nomes de atributo de esquema de LDAP em seu filtro. Sempre coloque seu filtro entre aspas duplas e use parênteses para esclarecer a ordem de precedência de operador.

Por exemplo, use o seguinte comando para pesquisar todos os registros em que sn=Account_10001:

```
pdm_ldap_test –f "(sn=Account_10001)"
```

O utilitário pdm_ldap_test oferece suporte aos seguintes operadores de igualdade:

Operador de igualdade	Descrição
=	igual a
<=	menor que ou igual a
>=	maior que ou igual a
~=	semelhante

O utilitário pdm_ldap_test oferece suporte aos seguintes operadores booleanos:

Operador booleano	Descrição
&	E
|	OU
!	NOT

Os operadores AND e OR afetam cada conjunto de parênteses () no filtro de pesquisa. O NOT afeta apenas o primeiro conjunto de parênteses. Sempre coloque esses operadores *antes* dos filtros de pesquisa que devem ser afetados, em vez de entre os filtros. Eles podem ser aplicados a qualquer quantidade de filtros, como mostra o seguinte exemplo:

```
"(&(sn=Brown)(initials=A)) "

"(|(sn=Brown)(sn=Smith))"

"(!sn=Brown)"
```

Determinar que Nomes de atributo têm Valores

Use o parâmetro -a "*" e o parâmetro -f com o comando pdm_ldap_test para determinar quais atributos estão definidos para os registros de Usuário ou Grupo do LDAP. Esse teste é útil para determinar se há atributos LDAP que você deseja mapear para atributos de Contato, e para verificar se um atributo particular tem um valor e deve estar disponível ao criar ou atualizar registros de contato.

O exemplo a seguir mostra a saída de um diretório iPlanet:

```
pdm_ldap_test -a "*" -f sn=Account_1000001

2 LDAP records found...

DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top

DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
    mail(28)(0): ThisIsTheMailingAddressField
    uid(13)(0): Login_1000001
    givenName(17)(0): GivenNameOfPerson
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top
```

O exemplo a seguir mostra a saída do Active Directory:

```
Ldap_test –a “*” –f (&(sn=Brown)(initials=A))”

1 LDAP records found...

DN: CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
    objectClass(3)(0): top
    objectClass(6)(1): person
    objectClass(20)(2): organizationalPerson
    objectClass(4)(3): user
    cn(16)(0): John A. Smith
    sn(5)(0): Brown
    givenName(7)(0): John
    initials(1)(0): A
    distinguishedName(55)(0): CN=John A.
    Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
    displayName(16)(0): John A. Smith
    memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
    sAMAccountName(7)(0): smijo04
    userPrincipalName(25)(0): smijo04@mydomain.xyz.com
    objectCategory(63)(0):
    CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,DC=com
```

Ligar o rastreamento de LDAP

Use o utilitário pdm_logstat para ligar o log de rastreamento para monitorar o uso de LDAP no CA SDM.

O comando pdm_logstat tem a seguinte sintaxe:

```
pdm_logstat -f ldap_virtdb.c 1000
```

As seguintes mensagens stdlog o ajudarão a entender o status do processo de conexão.

Determinar se o processo ldap_virtdb foi iniciado

A primeira linha a examinar quando analisar o stdlog em busca de mensagens de LDAP é o início do processo ldap_virtdb. O CA SDM só reconhece o LDAP quando esse processo é iniciado.

Observação: mesmo que opções de integração com LDAP não tenham sido instaladas nem configuradas, esse processo será executado.

```
06/03 17:00:18.27 cpasd1    bopLDAP       1964 SIGNIFICANT   ldap_virtdb.c

680 STARTUP of LDAP_virtdb
```

Determinar se todas as opções necessárias foram instaladas

Se qualquer uma das opções necessárias de LDAP não tiver sido definida, o stdlog mostrará as que estiverem ausentes, como ilustrado no exemplo a seguir:

```
06/03 17:00:18.72 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
port id missing
06/03 17:00:18.78 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name missing
06/03 17:00:18.78 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name password missing
```

Determinar se a conexão LDAP foi bem-sucedida

Você pode identificar se a conexão de LDAP é bem-sucedida verificando as entradas no stdlog. As entradas devem indicar que uma conexão com êxito foi estabelecida com o servidor LDAP, como ilustrado no exemplo a seguir:

```
06/05 12:35:10.41 cpasd1   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c  958 LDAP_SRVR
connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c 1002 LDAP_SRVR
binding with username(simon)
```

Determinar se a conexão LDAP não está disponível

Se uma conexão não puder ser estabelecida com o servidor LDAP por alguma razão, as funções *Entradas LDAP*, *Mesclar LDAP* ou qualquer outra função de LDAP será desconectada e não retornará nenhum resultado. Nesse caso, o stdlog mostra mensagens semelhantes às dos seguintes exemplos ao acessar essas operações:

```
06/03 17:00:32.25 cpasd1  bopLDAP  1964 SIGNIFICANT  ldap_virtdb.c   219 LDAP server
not available; 'register_producer' not processed

06/05 10:52:57.63 cpasd1  bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c   219 LDAP server
not available; 'select_full' not processed

06/05 10:52:57.66 cpasd1  web:local 1868 ERROR   sel_data_cache.  611 Error in ldap
Select_Cache method got_initial_count: LDAP server not available; 'select_full' not
processed

06/05 10:52:57.66 cpasd1  bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c   219 LDAP server
not available; 'select_cancel' not processed
```

Determinar o filtro real usado

O CA SDM busca registros do Diretório LDAP de acordo com a base de pesquisa e o filtro definido no Gerenciador de opções, bem como o critério de pesquisa digitado pelo usuário. Procure a seguinte mensagem para determinar o filtro real gerado na solicitação de pesquisa:

```
06/24 14:18:28.32 mcxxx04- bopLDAP   3844 TRACE   ldap_virtdb.c   853 Starting select
full: base=DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person)(|(sn=Jones)(pzLastName=Jones)));
attributes=(uid,sAMAccountName,pzUserName,distinguishedName)
```

Determinar atributos recuperados

O CA SDM busca registros do Diretório LDAP de acordo com a base de pesquisa e o filtro definido no Gerenciador de opções. Procure a seguinte mensagem para determinar se SEARCH_BASE e mapeamento de atributo definidos no ldap.maj e ldap_group.maj estão corretos:

```
06/24 14:18:28.39 mcxxx04- bopLDAP      3844 TRACE     ldap_virtdb.c    766 Starting
select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person));
attributes=(modifyTimestamp,sn,pzLastName,givenName,pzFirstName,initials,pzMiddle
Name,uid,sAMAccountName,pzUserName,telephoneNumber,pzWorkPhoneNumber,mobile,pzMob
ilePhoneNumber,department,pzDepartment,facsimileTelephoneNumber,pzFaxPhoneNumber,
pager,mail,pzEmailAddress,streetAddress,pzAddress,l,pzCity,st,pzState,postalCode,
pzPostalCode,c,pzCountry,o,memberOf)
```

Determinar que dados de LDAP estão disponíveis ou não

Supondo que o CA SDM tenha sido capaz de mapear para o atributo da ID do objeto LDAP com êxito, os atributos definidos em $NX_ROOT/bopcfg/majic/ldap.maj serão recuperados para cada entrada, ou uma mensagem será registrada indicando que um atributo não foi definido. Uma amostra dessas mensagens é mostrada a seguir:

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'modifyTimestamp'
```

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'telephoneNumber,pzWorkPhoneNumber'
```

Capítulo 6: Gerenciando funções

Observação: Para obter informações sobre outros aspectos da interface da web, consulte Configurando a interface da Web (na página 389).

Esta seção contém os seguintes tópicos:

Funções (na página 251)
Funções predefinidas (na página 251)
Segurança baseada em funções (na página 254)
Navegação com base em função (na página 264)
Como implementar uma função personalizada (na página 275)
Como implementar uma árvore de menu personalizada (na página 277)
Criar um registro de função (na página 279)
Criar um registro de guia (na página 280)
Criar um registro de barra de menu (na página 281)
Criar um registro de formulário Web (na página 282)
Copiar uma árvore de menus (na página 283)
Criar e personalizar uma árvore de menu (na página 284)
Criar e publicar um pacote de ajuda (na página 286)
Alternar funções (na página 288)

Funções

Funções são registros primários que controlam a segurança e a navegação da interface de usuário do CA SDM. Cada função define uma exibição concentrada do sistema, expondo somente a funcionalidade necessária para os usuários executarem as tarefas tipicamente atribuídas à função que executam dentro de sua organização.

A função padrão de um usuário determina a exibição de sistema que está presente no logon. Usuários com várias atribuições de função podem alternar de uma função para outra para visualizar diferentes exibições do sistema sem a necessidade de fazer logoff e logon novamente.

Funções predefinidas

Você pode usar as funções predefinidas em sua configuração padrão, modificá-las para que atendam a seus requisitos de negócios ou criar novas funções.

A tabela a seguir descreve as funções predefinidas instaladas com o CA SDM. Estas funções são projetadas para alinhamento com as melhores práticas do ITIL v3, reduzindo, assim, a quantidade de personalizações específicas do local necessárias para levar a conformidade com o ITIL à sua empresa de TI.

O CA SDM oferece suporte apenas ao ITIL, e a documentação do CA SDM é orientada pelo ITIL. Para obter mais informações, consulte Configuração do ITIL (na página 34).

Tipo da função	Nome da função	Descrição
Usuários finais	Visualizador de configuração	Realiza tarefas básicas de exibição e pesquisa de IC de dentro de sua organização.
	Cliente	Realiza tarefas básicas de autoatendimento de fora de sua organização.
	Funcionário	Realiza tarefas básicas de autoatendimento de dentro de sua organização.
Analistas	Analista de configuração	Realiza tarefas dentro do processo de ciclo de vida do item de configuração e suporte de segundo nível do CMDB dentro de sua organização.
	Representante do atendimento ao cliente	Oferece suporte aos usuários externos à sua organização, mais frequentemente clientes.
	Analista de conhecimento	Realiza tarefas dentro do processo de ciclo de vida do gerenciamento do conhecimento.
	Analista de nível 1	Oferece suporte de primeiro nível dentro de sua organização.
	Analista de nível 2	Oferece suporte de segundo nível dentro de sua organização, o que requer conhecimentos mais avançados do especialista no assunto.
	Analista da Support Automation	Oferece suporte de primeiro nível dentro de seu ambiente de assistência online.
	Analista de fornecedor	Oferece suporte a um segmento limitado de seu ambiente de TI de fora de sua organização, como um hardware específico de fornecedor.
Gerentes	Gerenciador de mudanças	Gerencia o processo de requisição de mudança, mas geralmente não o analista que trabalha com tickets de requisição de mudança.

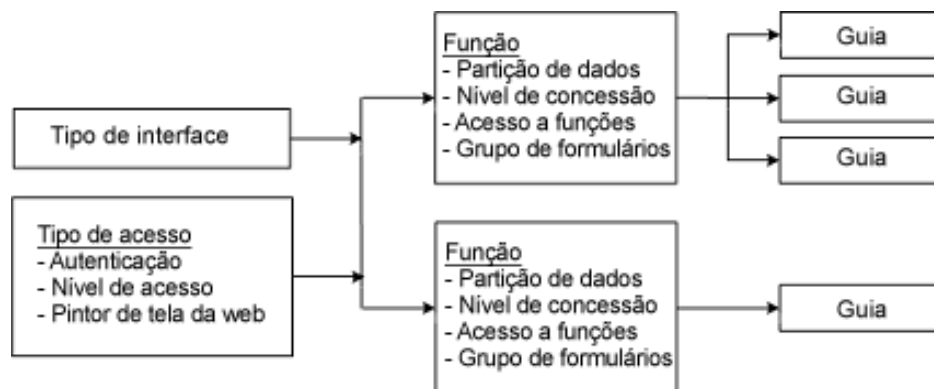
Tipo da função	Nome da função	Descrição
	Gerenciador de atendimento ao cliente	Gerencia Representantes de atendimento ao cliente e o processo de suporte externo.
	Gerente de incidentes	Gerencia o processo de incidente, mas geralmente não o analista que trabalha com tickets de incidente.
	Gerente de conhecimento	Supervisiona analistas de conhecimento, reatribuições e encaminhamento de documentos de conhecimento e administração de documentos do dia-a-dia.
	Gerenciador de problemas	Gerencia o processo de problema, mas geralmente não o analista que trabalha com tickets de problema.
	Service Desk Manager	Trata encaminhamentos e supervisiona Analistas de nível 1. Também pode gerenciar as operações gerais da central de serviço.
Administradores	Administrador	Executa tarefas administrativas por toda implementação do CA SDM e Gerenciamento de conhecimento. Esta função geralmente instala, configura e integra os produtos.
	Administrador de configuração	Realiza tarefas administrativas relacionas à implementação do CA CMDB. Esta função geralmente administra a infraestrutura do CMDB e de itens de configuração, e estruturas de dados.
	Administrador do gerenciamento de conhecimento	Configura e monitora definições de gerenciamento de conhecimento.
	Administrador do Service Desk	Realiza tarefas administrativas de dados e processos, como criação e atualização de categorias, contatos, tipos de serviço, causas raiz e assim por diante.
	Administrador de Support Automation	Realiza tarefas administrativas relacionadas a seu ambiente do Support Automation, como configuração de filas e permissões de ferramenta de analista.

Tipo da função	Nome da função	Descrição
	Administrador do sistema	Realiza tarefas administrativas relacionadas à implementação, configuração e adaptação do CA SDM, como opções de definição, configuração de integrações e modificação de formulários da Web.
	Administrador de inquilino	Realiza tarefas administrativas de multilocação específicas de um inquilino ou organização de suporte particulares.

Segurança baseada em funções

Tipos e funções de acesso são os componentes primários usados para controlar a segurança do CA SDM.

O diagrama a seguir mostra uma visão geral de como as funções se inter-relacionam com outros objetos de sistema para fornecer segurança com base em funções.

Observação: para obter mais informações sobre segurança de outros aspectos, consulte Segurança (na página 185).

Como funcionam os tipos de acesso

Cada tipo de acesso para um usuário controla os seguintes aspectos de comportamento do sistema:

- Como o CA SDM executa autenticação de web quando o usuário efetua logon
- O nível de acesso para o usuário

- Se o usuário pode modificar formulários web ou o esquema de banco de dados usando Web Screen Painter
- Quais funções estão disponíveis para o usuário

É possível associar um tipo de acesso a um contato, selecionando o tipo de acesso enquanto cria ou atualiza o registro de contato.

A tabela a seguir lista os tipos de acessos predefinidos, identifica suas funções vinculadas e fornece uma breve descrição.

Tipo de acesso	Funções vinculadas	Descrição
Administração	■ Administrador (padrão) ■ Administrador de configuração ■ Funcionário ■ Analista de nível 2 ■ Administrador do Service Desk ■ Administrador do sistema ■ Administrador de inquilino	Fornece acesso com o mais alto nível de segurança a todas as principais funções de administração. Usado durante implementação e administração em andamento. **Observação:** o tipo de acesso de Administração é pré-configurado para permitir que administradores alternem para qualquer função vinculada. Por exemplo, para visualizar uma exibição diferente do sistema, administradores podem alternar para a função Funcionário sem ter de efetuar logoff e logon novamente.
Cliente	■ Cliente	Fornece acesso altamente restrito a clientes *externos* que usam a exibição de autoatendimento.
Funcionário	■ Funcionário	Fornece acesso altamente restrito a funcionários *internos* que usam a exibição de autoatendimento. Usado para criar novo incidente e atualizar páginas de incidente.

Tipo de acesso	Funções vinculadas	Descrição
Equipe de TI	■ Analista de configuração ■ Funcionário ■ Analista de nível 2 (padrão) ■ Analista de conhecimento ■ Administrador do gerenciamento de conhecimento ■ Gerente de conhecimento	Fornece acesso voltado ao analista para usuários que trabalham dentro da organização de TI, mas que não são realmente membros da equipe de suporte. Esse acesso é destinado especificamente a usuários que precisam de acesso ao Gerenciamento de conhecimento.
Gerenciamento de conhecimento	■ Administrador de configuração ■ Analista de configuração ■ Visualizador de configuração ■ Funcionário ■ Analista de conhecimento ■ Administrador do gerenciamento de conhecimento (padrão) ■ Gerente de conhecimento ■ Analista de nível 2	Fornece acesso administrativo adaptado a usuários que administram recursos do Gerenciamento de conhecimento.
Gerenciamento de processos	■ Gerenciador de mudanças ■ Analista de configuração ■ Funcionário ■ Gerenciador de incidentes (padrão) ■ Analista de nível 2 ■ Gerenciador de problemas ■ Service Desk Manager	Fornece acesso adaptado a usuários que executam as principais funções de gerenciamento de processo.

<table>
<tr><th>Tipo de acesso</th><th>Funções vinculadas</th><th>Descrição</th></tr>
<tr><td>Gerenciamento do Service Desk</td><td>■ Gerenciador de atendimento ao cliente
■ Analista de configuração
■ Funcionário
■ Analista de nível 1
■ Analista de nível 2
■ Service Desk Manager (padrão)</td><td>Fornece acesso adaptado a usuários que gerenciam suporte de TI ou funções de atendimento a cliente externo (normalmente supervisores de suporte de primeiro nível).</td></tr>
<tr><td>Equipe do Service Desk</td><td>■ Analista de configuração
■ Visualizador de configuração
■ Representante do atendimento ao cliente
■ Funcionário
■ Analista de nível 1 (padrão)
■ Analista de nível 2</td><td>Fornece acesso adaptado a usuários que executam tarefas de suporte. O acesso é concentrado nos usuários que executam suporte de primeiro nível.</td></tr>
<tr><td>Admin da Support Automation</td><td>■ Administrador de Support Automation</td><td>Fornece acesso a usuários que executam administração de Support Automation.</td></tr>
<tr><td>Analista da Support Automation</td><td>■ Analista da Support Automation</td><td>Fornece acesso a usuários que prestam assistência online a usuários finais.</td></tr>
<tr><td>Equipe do fornecedor</td><td>■ Analista de fornecedor</td><td>Fornece acesso altamente restrito a fornecedores externos, que trabalham somente com itens diretamente relacionados a seu produto (por exemplo, uma marca específica de hardware).</td></tr>
</table>

Registros de função

É possível atribuir funções para um tipo de acesso, ou diretamente a um registro de contato do usuário. Se um conflito de atribuição de função ocorrer, as atribuições da função do contato têm precedência.

Cada registro de função deve ser configurado com os seguintes componentes:

- Um grupo de formulários
- Um tipo de interface de usuário
- Configurações de acesso da função
- Uma ou mais guias
- Um conjunto de ajuda

Os seguintes componentes opcionais também podem contribuir para cada definição de função:

- Árvores de menus
- Gerenciadores de filas
- Barras de menu
- Barras de ferramentas
- Uma partição de dados
- Acesso ao Gerenciamento de conhecimento
- Níveis de acesso do Support Automation
- Formulários web de relatório
- Recursos Ir

Áreas de acesso funcional

Áreas de acesso funcional definem o acesso de nível de função para registros de ticket e outros componentes de sistema. A tabela usp_functional_access_type define a área e as tabelas usp_functional_access_level descrevem o acesso do usuário.

A tabela a seguir mostra as áreas de acesso funcional padrão:

Nome	Nome de código	Novo
Administração	admin	Não
Incidente/Problema/Solicitação	call_mgr	Não
Requisição de mudança	change_mgr	Não
Inventário	inventário	Não
Ocorrência	issue_mgr	Não
Documento de conhecimento	kd	Não
Notificação	notify	Não
Referência	referência	Não
Segurança	security	Não
Anúncio	anúncio	Sim
Referência do incidente/problema/solicitação	call_mgr_reference	Sim
Modelo do incidente/problema/solicitação	call_mgr_template	Sim
Modelo de requisição de mudança	change_mgr_template	Sim
Referência da requisição de mudança	change_reference	Sim
Item de configuração	ic	Sim
Item de configuração comum de somente leitura	ci_common_ro	Sim
Referência de item de configuração	ci_reference	Sim
Contato	contato	Sim
Grupo	group	Sim
Modelo de ocorrência	issue_mgr_template	Sim
Referência da ocorrência	issue_reference	Sim
Local	location	Sim

Administração de vários sites	multisite_admin	Sim
Referência de vários sites	multisite_reference	Sim
Referência de notificação	notification_reference	Sim
Organização	organização	Sim
Priorização	prioritization	Sim
Nível do serviço	service_level	Sim
Site	site	Sim
Consulta armazenada	stored_queries	Sim
Support Automation	sa	Sim
Pesquisa	pesquisa	Sim
Administração de inquilinos	tenant_admin	Sim
Fuso horário	timezone	Sim
Referência de fluxo de trabalho	workflow_reference	Sim
Turno de trabalho	turnos de trabalho	Sim

Como adicionar uma área de acesso funcional

Quando você adiciona uma área de acesso funcional, as funções existentes automaticamente têm acesso de Modificar. Você pode revisar e alterar os níveis de acesso para conceder a autoridade adequada.

Para adicionar uma área de acesso funcional, faça o seguinte:

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Acesso funcional.
2. Clique em Criar novo.

   A página da Lista Criar acesso funcional aparece.
3. Complete os campos da área de acesso funcional conforme o adequado.
4. Clique em Salvar.

   A página Detalhes do Acesso Funcional aparece.
5. Aplicar níveis de acesso a uma (na página 263) ou mais (na página 261) funções.

Observação: para informações detalhadas sobre áreas de acesso funcional, consulte a *Ajuda online.*

Aplicar níveis de acesso a muitas funções

Para uma área de acesso funcional, você pode definir os níveis de acesso para cada função para economizar tempo. Em vez de usar Gerenciamento de função, você atualiza a área de acesso funcional com os níveis de acesso de função adequados.

Para aplicar níveis de acesso a muitas funções, faça o seguinte:

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Acesso funcional.
2. Clique no nome da área da função.
3. Na guia Funções, clique em Editar na Lista.
4. Revise e atualize cada função conforme o adequado. Os seguintes níveis de acesso estão disponíveis:

   Nenhuma

   Nega o acesso de função ao objeto de função.

   Exibir

   Concede capacidade apenas de leitura ao objeto de função.

   Modificar

   Concede capacidade de leitura/gravação ao objeto de função.
5. Continue selecionando funções e níveis de acesso.
6. (Opcional) Clique em Alterar todos.
7. Clique em Salvar.

   As mudanças às funções aplicam-se imediatamente.

Observação: para informações sobre funções e níveis de acesso funcional, consulte a *Ajuda online.*

Exemplo: alterar os níveis de acesso para o anúncio

Esse exemplo mostra como você pode definir níveis de acesso de função para a área de acesso funcional Anúncio.

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Acesso funcional.

   A página Detalhes do Acesso Funcional aparece.

2. Clique em Anúncio.
3. Na guia Funções, clique em Editar na Lista.
4. Selecione Analista de nível 2
5. Selecione View from the Access Level.

   O nível de acesso para a função Analista de nível 2 é destacado com o valor de Exibir.
6. Selecione Analista de configuração.
7. Selecione Modificar no Nível de acesso.

   O Nível de acesso para o Analista de configuração destaca-se com o valor de Modificar.
8. Clique em Salvar.

   Uma mensagem confirma a mudança.
9. Efetue logon como uma função de Analista de nível 2.
10. Selecione Exibir anúncios.

    A página Anúncios aparece.
11. Clique em um anúncio.

    Uma mensagem lembra você de que, como Analista de nível 2, você somente pode visualizar anúncios.
12. Configurar a função para Analista de configuração.
13. Selecione Exibir anúncios.

    A página Anúncios aparece.
14. Clique em um anúncio.

    A página Atualizar anúncio é exibida. Como um Analista de configuração, você pode modificar anúncios.

Aplicar um nível de acesso a uma função

Você pode usar Gerenciamento de função para alterar a maneira como os usuários acessam a interface com o usuário. Quando você altera os níveis de acesso para uma função, a interface com o usuário exibe somente objetos, páginas e itens de menu com base no nível de acesso. Por exemplo, se uma função não puder mais criar contatos, o menu Arquivo omite Novos contatos.

Para aplicar um nível de acesso a uma função, faça o seguinte:

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Gerenciamento das funções, Lista de funções.
2. Na Lista de funções, clique com o botão direito do mouse no nome da função e selecione Editar no menu de atalho.
3. Clique em Editar na Lista na guia Acesso a funções.
4. Clique em um nome de função.

   A linha se destaca.
5. Atualize as áreas de acesso funcional com os seguintes níveis de acesso conforme o adequado:

   Nenhuma

   Nega o acesso de função ao objeto de função.

   Exibir

   Concede capacidade apenas de leitura ao objeto de função.

   Modificar

   Concede capacidade de leitura/gravação ao objeto de função.
6. Clique em Salvar.

   Uma mensagem confirma a mudança. A função pode imediatamente usar a área de acesso funcional no nível de acesso especificado.
7. Verifique o nível de acesso efetuando logon como a função e verificando menus, opções de página e botões.

Exemplo: conceder a Função de analista de nível 2 modifica acesso aos tickets

Este exemplo mostra como a interface do usuário muda quando você concede a um Analista de nível 2 acesso para modificar tickets.

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Gerenciamento das funções, Lista de funções.

   A Lista de funções aparece.

2. Clique com o botão direito do mouse em Analistas de nível 2 e selecione Editar a partir do menu de atalho.
3. Clique em Editar na Lista na guia Acesso a funções.
4. Selecione Referência do incidente/problema/solicitação.
5. Selecione Modificar no Nível de acesso.

   O nível de acesso atualiza para Modificar.

6. Clique em Salvar e efetue logoff.

   Uma mensagem confirma a mudança.

7. Efetue logon como uma função de Analista de nível 2.
8. Selecione Pesquisar, Incidentes.
9. Clique em Pesquisar e abra um incidente.

   A página Detalhes do incidente inclui um botão Editar na Lista. Como um Analista de nível 2, é possível modificar o ticket.

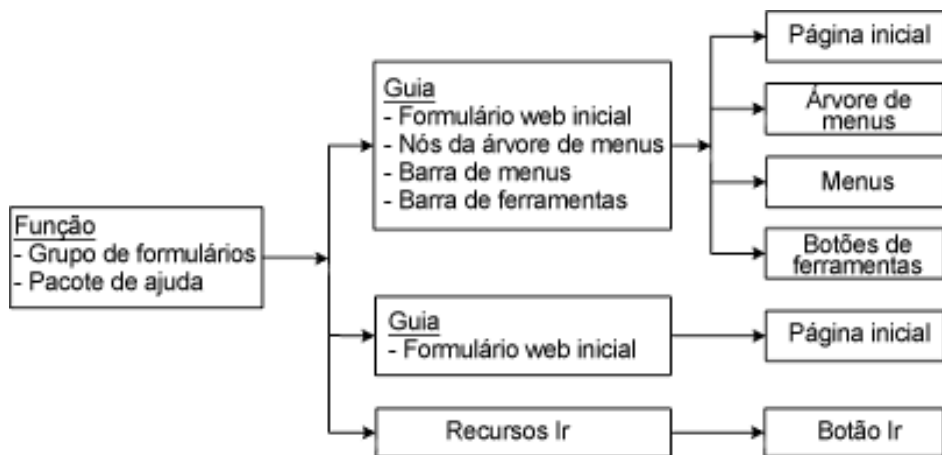
Partições de dados

As partições de dados são subconjuntos do banco de dados do CA SDM que permitem controlar o acesso no nível de registro. É possível associar uma partição de dados a uma função para controlar acesso a tickets e outros registros que podem ser acessados por meio da interface da Web.

Para obter informações sobre o trabalho com partições de dados, consulte Associações de partição de dados (na página 203).

Navegação com base em função

A exibição da interface da Web para cada usuário é definida por uma função. Usuários com várias atribuições de função podem alternar entre diversas exibições de interface da Web.

O diagrama a seguir mostra como as funções se inter-relacionam com outros objetos para produzir uma apresentação da interface com o usuário com base na função.

Guias

Uma guia é uma entidade de exibição gráfica que se vincula a uma função para apresentar recursos para os usuários dessa função. Quando um usuário faz logon no sistema, a janela principal exibe as guias atribuídas à função padrão do usuário.

As guias definem as subdivisões principais na janela principal da interface da web. Cada guia é configurada para expor um conjunto apropriado de recursos de interface de usuário às funções que os usam.

Todas as funções devem ter pelo menos uma guia. Você pode associar uma ou mais guias a uma função. Cada guia tem um número de seqüência que controla sua requisição de exibição na janela principal. Se apenas uma guia estiver associada a uma função, a página inicial da guia será exibida, não a guia.

Você pode configurar guias para incluir os seguintes tipos de recursos de exibições:

- Uma página inicial (formulário web padrão) é exibida quando um usuário seleciona a guia. A página inicial é um elemento necessário de todas guias. Você pode atribuir somente uma página inicial a cada guia.

  Observação: é possível configurar uma página inicial para exibir relatórios gráficos a partir de Objeto de negócio, que permite que os usuários gerem relatórios em tempo de execução. Para obter mais informações, consulte Geração de relatórios do CA Business Intelligence (na página 829).

- Uma barra de menus, que apresenta listas suspensas de comandos, como os comandos Arquivo, Exibir e Pesquisar. A barra de menus é opcional. Você pode atribuir somente uma barra de menus a cada guia.
- Uma barra de ferramentas, que apresenta botões de ferramentas para fácil acesso a comandos de menu usados frequentemente. A barra de ferramentas é opcional.

O CA SDM fornece várias guias predefinidas. Você pode atribuir as guias predefinidas a uma função, modificar as guias predefinidas e criar guias personalizadas.

Importante: Não atribua mais guias do que seu navegador pode exibir, pois isto fará com que guias com números de sequência mais altos sejam posicionadas além da exibição visível da janela e torná-las inacessíveis ao usuário.

Importante: Inclui somente guias que contenham formulários que estão incluídos no grupo de formulários atribuído à função que você está criando ou editando. Por exemplo, não atribua a guia Cliente nem a guia Funcionário à função de Administrador; fazer isso causará um erro quando os usuários tentarem acessar essas guias. O grupo de formulários da função é especificado no campo Grupo de formulários de personalização na página Detalhes da função, e também é exibido na coluna Grupo de formulários, na página Lista de funções. Para obter uma lista de formulários da web em cada grupo de formulário, consulte Grupos de formulário (na página 1209).

Guias predefinidas

A tabela seguinte mostra as guias predefinidas atribuídas a cada função. As guias são listadas em sequência de número, indicando sua posição na janela, da esquerda para a direita.

Observação: em muitos casos, existem várias versões de guias com o mesmo nome de exibição. Por exemplo, a guia Service Desk para a função Administrador fornece acesso completo à funcionalidade do CA SDM, enquanto que a guia Service Desk da função Gerenciador de mudanças tem foco maior em requisições de mudança.

Função	Guias
Administrador	■ Guia Service Desk com menu e gerenciador de filas completos ■ Guia Conhecimento ■ Guia Administração com a árvore de menu completa ■ Guia Relatórios - administrador ■ Guia Calendário de mudanças ■ Guia CA CMDB ■ Guia Support Automation
Gerenciador de mudanças	■ Guia Relatórios - gerenciador de mudanças ■ Guia Service Desk - gerenciador de mudanças ■ Guia Calendário de mudanças
Administrador de configuração	■ Guia CA CMDB ■ Guia Administração - administrador de configuração
Analista de configuração	■ Gerenciador de filas do CA CMDB - Analista de configuração
Visualizador de configuração	■ Gerenciador de filas do CA CMDB - Visualizador de configuração
Cliente	■ Guia Cliente
Gerenciador de atendimento ao cliente	■ Guia Service Desk - gerenciador de atendimento ao cliente ■ Guia Conhecimento ■ Guia Relatórios - Gerenciador de atendimento ao cliente

Função	Guias
Representante do atendimento ao cliente	■ Guia Service Desk - representante do atendimento ao cliente ■ Guia Perfil resumido ■ Guia Conhecimento
Funcionário	■ Guia Funcionário
Gerente de incidentes	■ Guia de relatórios - Gerenciador de incidentes ■ Guia do Service Desk - gerenciador de incidentes ■ Guia Conhecimento
Analista de conhecimento	■ Guia Service Desk - analista de conhecimento ■ Guia Conhecimento ■ Cronograma de gerenciamento de conhecimento ■ Guia Ficha de relatório de documento de conhecimento ■ Guia Relatórios - Analista de conhecimento
Gerente de conhecimento	■ Guia Service Desk - gerenciador de conhecimento ■ Guia Conhecimento ■ Cronograma de gerenciamento de conhecimento ■ Guia Administração - gerenciador de conhecimento ■ Guia Ficha de relatório de documento de conhecimento ■ Guia Relatórios - Gerenciador de conhecimento
Administrador do gerenciamento de conhecimento	■ Guia Administração - administrador de conhecimento
Analista de nível 1	■ Guia Service Desk - analista de nível 1 ■ Guia Perfil resumido ■ Guia Conhecimento
Analista de nível 2	■ Guia Service Desk - analista de nível 2 ■ Guia Conhecimento ■ Guia Calendário de mudanças
Gerenciador de problemas	■ Guia de relatórios - Gerenciador de problemas ■ Guia do Service Desk - gerenciador de problemas ■ Guia Conhecimento

Função	Guias
Administrador do Service Desk	■ Guia Administração - administrador do Service Desk
Service Desk Manager	■ Guia Relatórios - Service Desk Manager ■ Guia Service Desk - Service Desk Manager ■ Guia Conhecimento ■ Guia Calendário de mudanças
Administrador de Support Automation	■ Guia Service Desk - analista de nível 1 ■ Guia Support Automation ■ Admin da Support Automation ■ Guia Perfil resumido ■ Guia Conhecimento
Analista da Support Automation	■ Guia Service Desk - analista de nível 1 ■ Guia Support Automation ■ Guia Perfil resumido ■ Guia Conhecimento
Administrador do sistema	■ Guia Administração - administrador do sistema
Administrador de inquilino	■ Guia Administração - administrador de inquilino
Analista de fornecedor	■ Guia Service Desk - analista de fornecedor

Formulários web

Formulários Web definem as páginas que são exibidas na interface da web do CA SDM.

Existem quatro tipos de formulários da web:

- URL de Relatório de objeto de negócio
- Página HTMPL
- Recurso Ir
- Personalizado (por exemplo, um URL para uma página da web de terceiros)

Para obter informações sobre a criação de formulários da web personalizados, consulte Criar um registro de formulário da Web (na página 282).

Grupos de formulários

Os grupos de formulários definem os conjuntos de páginas na interface da web do CA SDM que estão disponíveis para uma função. Cada função tem um grupo de formulários. Os usuários só podem exibir as páginas da web incluídas no grupo de formulários atribuídos a sua função.

Cada tipo de interface tem um grupo de formulário associado um conjunto de arquivos HTMPL que definem as páginas que usuários com esse tipo de interface podem ver.

O CA SDM fornece os seguintes grupos de formulário predefinidos:

- Analista
- Cliente
- Funcionário
- ITIL

Você pode usar os grupos de formulário predefinidos na configuração padrão deles, modificar os grupos de formulário predefinidos e criar novos grupos de formulário usando o Pintor de tela da web. Você pode visualizar uma listagem dos nomes de arquivo HTMPL inclusos em cada grupo de formulário (na página 1209) predefinido.

Árvores de menus

As árvores de menus são listas hierárquicas de nós (recursos de árvores do menu) que são exibidos no painel de navegação à esquerda da janela principal da interface da web.

Uma função pode ter uma árvore de menu, que fornece nós para acesso a muitas áreas funcionais do sistema. Por exemplo, a função de Administrador predefinida tem uma árvore de menu que inclui nós para os recursos de administração de Sistema e Gerenciamento de Funções, recursos de administração do Service Desk e muitos outros.

Para funções que incluem uma árvore de menus, a árvore de menus fornece acesso a um conjunto de recursos especificado que fornece acesso a áreas funcionais do sistema.

O CA SDM fornece árvores de menu predefinidas para as seguintes funções:

- Administrador (admin_tree)
- Administrador do CA CMDB (cmdb_adm_tree)
- Administrador do gerenciamento de conhecimento (kt_adm_tree)
- Gerenciador de conhecimento (kt_mgr_tree)
- Support Automation Administrador (sa_admin_tree)
- Administrador do Service Desk (sd_adm_tree)
- Administrador do sistema (sys_adm_tree)
- Administrador do inquilino (tn_admin_tree)

Você pode editar os campos Nome, Status do registro e Descrição dos registros da árvore de menu predefinidos, mas não pode personalizá-los adicionando ou removendo seus recursos da árvore de menu.

Para personalizar uma árvore de menus, você pode criar um novo registro de árvore de menus ou copiar e personalizar uma das árvores de menus predefinidas.

Observação: o campo Interno não modificável em cada registro de árvore de menus indica se a árvore de menus pode ser personalizada. Um valor SIM no campo Interno indica uma árvore de menus predefinida, que não pode ser personalizada. Um valor NÃO indica uma árvore de menus definida na localidade, que pode ser personalizada. O botão Personalizar menu aparece somente em registros de detalhes de árvore de menus com um valor do campo Interno de NÃO.

Quando você anexa uma árvore de menus a uma guia, ela torna-se disponível a todas funções com acesso a essa guia.

Recursos de árvores do menu

Recursos da árvore de menus definem os itens que os usuários podem acessar a partir da árvore.

Um recurso de árvore de menus consiste em um nome, sua descrição e um fragmento de URL ou nome do arquivo HTPML usado pelo mecanismo da web que controla a página da web exibida.

Barras de menu

Uma barra de menu é um elemento útil da interface do usuário que exibe uma lista horizontal de menus na janela principal da interface da Web. Cada menu contém uma lista suspensa de opções ou comandos. Você pode definir barras de menu personalizadas para quaisquer funções personalizadas que possa criar.

Registros da barra de menus especificam o formulário HTMPL que controla os itens de menu que a barra de menu pode acessar.

Observação: para definir a funcionalidade da barra de menus, você deve usar o aplicativo Pintor de tela da web. Para obter informações sobre a configuração da funcionalidade de uma barra de menus predefinida ou personalizada, consulte a *Ajuda online do Pintor de tela da web*.

A tabela a seguir lista as barras de menu predefinidas e identifica as guias predefinidas que as usam.

Barra de menus	Guias associadas
Administração	■ Guia Administração - administrador de configuração ■ Guia Administração - administrador de conhecimento ■ Guia Administração - gerenciador de conhecimento ■ Guia Administração - administrador do Service Desk ■ Guia Administração - administrador do sistema ■ Guia Administração - administrador de inquilino ■ Guia Administração com a árvore de menu completa
CA CMDB	■ A guia do CA CMDB com o menu completo e o gerenciador de filas
Calendário de mudança	■ Guia Calendário de mudanças

Barra de menus	Guias associadas
Conhecimento	■ Guia Conhecimento ■ Cronograma de gerenciamento de conhecimento
Service Desk	■ Guia Service Desk com menu e gerenciador de filas completos
Service Desk - gerenciador de mudanças	■ Guia Service Desk - gerenciador de mudanças
Service Desk - gerente do atendimento ao cliente	■ Guia Service Desk - gerenciador de atendimento ao cliente
Service Desk - representante do atendimento ao cliente	■ Guia Service Desk - representante do atendimento ao cliente
Service Desk - gerenciador de incidentes	■ Guia do Service Desk - gerenciador de incidentes
Service Desk - analista de conhecimento	■ Guia Service Desk - analista de conhecimento
Service Desk - gerenciador de conhecimento	■ Guia Service Desk - gerenciador de conhecimento
Service Desk - analista de nível 1	■ Guia Service Desk - analista de nível 1
Service Desk - analista de nível 2	■ Guia Service Desk - analista de nível 2
Service Desk - gerenciador de problemas	■ Guia do Service Desk - gerenciador de problemas
Service Desk - gerenciador do Service Desk	■ Guia Service Desk - Service Desk Manager
Service Desk - analista de fornecedor	■ Guia Service Desk - analista de fornecedor
Support Automation - analista	■ Guia do Support Automation - analista do Support Automation

Barras de ferramentas

Barras de ferramentas ampliam a funcionalidade das barras de menu adicionando a capacidade de exibir um ou mais botões de ferramentas à direita dos menus.

Botões de ferramenta aparecem como ícones na barra de ferramentas. Clicar em um botão de ferramenta fornece ao usuário acesso fácil para opções ou comandos de menu usados com frequência.

Observação: o aplicativo Pintor de tela da Web é usado para definir a funcionalidade da barra de ferramentas. Para obter mais informações sobre a configuração da funcionalidade de uma barra de ferramentas predefinida ou personalizada, consulte a *Ajuda online do Pintor de tela da Web*.

Recursos Ir

O botão *Ir* fornece um meio fácil de localizar um registro em particular.

Os recursos Ir são um tipo de formulário da Web. Se uma função possui recursos Ir associados, quando um usuário efetua logon com essa função, o botão Ir aparece no canto superior direito da janela principal do CA SDM e em todas as janelas pop-up. O botão Ir possui dois campos associados na interface do usuário:

- Uma lista suspensa para selecionar o tipo de registro a pesquisar (por exemplo, Requisição de mudança)
- Uma caixa de texto para inserir um valor para identificar um registro em particular (por exemplo, 135 para localizar a Requisição de mudança 135)

Atribuindo recursos Ir a uma função, é possível especificar os tipos de registros que os usuários nessa função podem pesquisar. Por exemplo, a função de Administrador predefinida possui os seguintes recursos Ir:

- Requisição de mudança
- Documento por ID
- Incidente
- Ocorrência
- Conhecimento
- Problema
- Solicitação

- Usuário por ID
- Usuário por nome
- Usuário por telefone

Pacotes de ajuda

Pacotes de ajuda são as coleções de tópicos de ajuda online disponíveis para os usuários, dependendo das atribuições de sua função e da configuração da função atual. Se você efetuar logon usando a função de Administrador, por exemplo, poderá exibir os tópicos de ajuda online incluídos no pacote de ajuda de Administrador. Se alternar para a função de Funcionário, você poderá exibir o pacote de ajuda de Funcionário.

Cada função predefinida tem um pacote de ajuda predefinido correspondente. Você pode criar conjuntos de ajuda personalizados para quaisquer funções que possa definir.

Observação: para obter informações sobre trabalhar com definições de pacote de ajuda, consulte a *Ajuda Online*.

Como implementar uma função personalizada

Para muitos locais, as funções predefinidas são suficientes. Pode haver situações, entretanto, em que você deseja criar uma função personalizada e projetá-la para atender necessidades de negócio específicas do local na organização.

O seguinte processo destaca as tarefas necessárias ao implementar uma nova função. O exemplo mostrado aqui descreve como você poderia implementar uma função para um pequeno grupo de analistas com tarefas de revisar e autorizar tickets de requisição de mudança.

Para implementar uma função personalizada, realize as tarefas descritas no seguinte exemplo:

1. Criar um novo registro de função usando os seguintes valores de campo:

   Nome da função

   Analista de mudanças

   Código

   chg_anal

Grupo de formulários de personalização

Analista

Documento preferencial

Incidente

2. Selecione o Analista do Service Desk no campo Partição de dados na guia Autorização.
3. Selecione Modificar no campo Requisições de mudança na guia Acesso a funções.
4. Insira os seguintes valores na guia Interface da Web:

   Tipo de interface de usuário da Web

   Analista

   Exibição da ajuda

   Analista de mudanças

5. Selecione as seguintes guias:
   - Guia Relatórios - analista de mudanças
   - Guia Service Desk - analista de mudanças
   - Guia Calendário de mudanças
6. Selecione os seguintes relatórios na guia Formulários web de relatório:
   - Relatório Vencimento das requisições de mudança ativos por prioridade para status
   - Requisições de mudança ativas no final da semana
   - Requisições de mudança por tipo de serviço com falha para categorias de mudança
7. Adicionar o recurso de Requisição de mudança na guia Recursos Ir.
8. Criar um conjunto de ajuda personalizada chamado Analista de mudança que inclui todos os conteúdos adequados para a nova função.

   Para obter mais informações, consulte Criar e publicar um pacote de ajuda (na página 286).

9. Criar as seguintes guias personalizadas usando os recursos adequados para a nova função:
   - Guia Relatórios - analista de mudanças
   - Guia Service Desk - analista de mudanças
10. Criar uma árvore de menu personalizada que inclua todos os nós adequados para a nova função.

    Para obter mais informações, consulte Como implementar uma árvore de menu personalizada (na página 277).

Como implementar uma árvore de menu personalizada

Para muitos locais, as árvores de menus predefinidas são suficientes. No entanto, pode haver situações em que você queira personalizar uma função, implementando uma árvore de menus personalizada para ela.

Na maioria dos casos, é mais fácil iniciar com uma cópia de uma árvore de menus predefinida e, em seguida, adicionar, remover ou reorganizar nós dentro da hierarquia. Como alternativa, é possível criar uma árvore de menus e construir uma hierarquia de nós totalmente nova.

Você pode usar cada um dos métodos a seguir para disponibilizar uma árvore de menus personalizada para uma função:

- Substitua a árvore de menus no formulário web (Página Inicial) pela guia que exibe o admin_tree original.
- Crie um formulário web e anexe o novo formulário web com a nova árvore de menus em uma guia.

Para implementar um menu personalizado, execute as seguintes tarefas:

1. Copie uma das árvores de menu predefinidas.

   Observação: faça uma observação do valor inserido no campo Código.

2. Crie um formulário web usando os seguintes valores de campo:

   - **Tipo:**HTMPL
   - **Recurso:**

     ```
     $cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=admin_main_role.htmpl
     +KEEP.tree_code=menu_tree_code
     ```

     Observação: especifique o valor do código para a árvore de menus criada na Etapa 1 para menu_tree_code. O código admin_main_role.htmpl usa o valor da variável KEEP.tree_code como sua árvore de menus.

3. Crie um registro de guia usando os seguintes valores de campo:

   - **Página inicial:** o formulário web criado na Etapa 2
   - **Barra de menus:** administração

   Observação: administração é uma barra de menus genérica usada por muitas funções, não é específica da função.

4. Atribua a guia criada na Etapa 3 à função que deseja que tenha acesso à árvore de menus personalizada.

5. Efetue logoff do CA SDM e efetue o logon novamente.

   A guia Administração exibe sua árvore de menus personalizada.

Mais informações:

Criar um registro de formulário Web (na página 282)

Criar um registro de função

Os administradores podem criar funções personalizadas para atender requisitos de negócios específicos do local.

Para criar uma função

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Lista de funções na guia Administração.

   A página Lista de funções aparece.

2. Clique em Criar novo.

   A página Criar função aparece.

3. Preencha os seguintes campos:

   Nome da função

   Especifica o nome que identifica a função onde quer que ela apareça na interface de usuário.

   Código

   Especifica um código que identifica a função para o sistema.

   Observação: após você salvar o registro, este valor de campo não poderá ser alterado.

   Status do registro

   Indica se a função está ativa ou inativa.

   Padrão?

   Indica se esta é a função padrão.

   Grupo de formulários de personalização

   Especifica um grupo de formulários predefinido ou personalizado.

   Documento preferencial

   Especifica o documento usado por esta função para inserir tickets no sistema.

Descrição

Descreve o propósito da função. Esta descrição aparece na página Lista de funções e pode facilitar a tarefa de atribuir usuários às funções apropriadas.

Clique em Salvar.

A definição de função é salva e a página Detalhes da função aparece.

Criar um registro de guia

Você pode criar guias personalizadas para serem exibidas na página principal da interface da Web. Quando você vincula um registro de guia a um registro de função, ele é disponibilizado aos usuários designados à função.

Para criar uma guia

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Guias na guia Administração.

   A página Lista de guias aparece.

2. Clique em Criar novo.

   A página Criar guia aparece.

3. Preencha os seguintes campos:

   Nome da guia

   Especifica o nome que identifica a guia dentro da interface administrativa. Por exemplo, o nome da guia aparece na página Lista de guias.

   Código

   Especifica o código que identifica a guia para o sistema.

   Observação: uma vez definido, o código não pode ser alterado.

   Status do registro

   Indica se a guia está ativa ou inativa.

   Nome de exibição

   Especifica o nome que aparece na apresentação gráfica da guia na interface de usuário.

Página inicial

Especifica o formulário web inicial que aparece na janela principal quando um usuário seleciona essa guia.

Importante: A Página inicial e a barra de menus devem pertencer ao mesmo grupo de formulários. Definir uma guia com uma página inicial e uma barra de menus que pertencem a grupos de formulários (na página 1209) diferentes causa um erro quando os usuários acessarem a guia.

Barra de menus

Especifica a barra de menus que aparece na janela principal quando um usuário seleciona essa guia.

Clique em Salvar.

A guia é criada.

Criar um registro de barra de menu

Você pode criar barras de menu personalizadas para controlar o acesso à funcionalidade do sistema para as funções definidas pelo usuário.

Para criar uma barra de menus

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Barras de menu.

   A página Lista de barras de menu é exibida.

2. Clique em Criar novo.

   A página Criar nova barra de menu é exibida.

3. Preencha os seguintes campos:

   Nome da barra de menu

   (Obrigatório) Especifica o nome que identifica a barra de menus. Você pode usar este campo para ajudar a identificar a funcionalidade disponível na barra de menus.

   Código

   (Obrigatório) Especifica o código que identifica esta barra de menus para o produto. Após definido, o código não pode ser alterado.

   Status do registro

   Indica se a barra de menus está ativa ou inativa.

Nome do HTMPL

Especifica o nome do formulário HTPML que contém a definição da barra de menus. A barra de menu é projetada usando o Web Screen Painter.

Descrição

Descreve a barra de menus. Use esta descrição para identificar melhor esta barra de menu e as funções que a usam.

Clique em Salvar.

A definição da barra de menu é salva e a página Detalhe da barra de menu aparece.

Criar um registro de formulário Web

Os administradores podem criar formulários web personalizados para serem as páginas iniciais para guias, relatórios para exibir em guias, recursos de botão Ir ou outro URL.

Para criar um formulário web

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Formulários web.

   A página Lista de formulários web é exibida.

2. Clique em Criar novo.

   A página Criar novo formulário web aparece.

3. Preencha os seguintes campos:

   Nome do formulário web

   (Obrigatório) Especifica o nome que identifica o formulário web.

   Status do registro

   Indica se este formulário está ativo ou inativo.

   Código

   (Obrigatório) Especifica o código que identifica o formulário web para o sistema. Após definido, o código não pode ser alterado.

   Observação: esse campo especifica o web_form_name na guia Propriedades para um formulários de quadros variados no Pintor de tela da web.

Tipo

Especifica um dos seguintes tipos de formulários web que você está criando:

- **Página HTPML** — Exibe uma página da web para ser usada como a página inicial para uma das guias personalizadas criadas por você.
- **Relatório** — Especifica um relatório do CA SDMexibido em qualquer guia.
- **Recurso Ir** — Especifica um recurso "Botão Ir".
- **Outro** — Acessa qualquer outra página da web externa por URL.

Descrição

Descreve o formulário web. Use essa descrição para melhor identificar esse formulário web, onde ele aparece e qual é a sua finalidade.

Recurso

Especifica o código que chama o formulário web. Esse código pode ser um código de linha de comando ou um URL.

Exemplo: Abrir um formulário htmpl simples "menu_tab_dflt.htmpl":

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=menu_tab_dflt.htmpl
```

Clique em Salvar.

Copiar uma árvore de menus

É possível copiar uma árvore de menus existente para usá-la como um ponto inicial para uma árvore de menus personalizada.

Para copiar uma árvore de menus

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Árvores do menu na guia Administração.

   A página Lista de árvores de menus aparece.

2. Clique na Árvore de menus para copiar.

   A página Detalhes da árvore de menu aparece.

3. Clique em Arquivo, Copiar.

   A página Criar árvore de menus aparece.

4. Preencha os seguintes campos:

   Nome da árvore do menu

   (Obrigatório) Especifica o nome atribuído que identificará a árvore do menu.

   Código

   (Obrigatório) Especifica o código que identifica a árvore do menu para o sistema. Após definido, o código não pode ser alterado.

   Status do registro

   Indica se a árvore de menus está ativa ou inativa.

   Descrição

   Descreve a árvore do menu. A descrição pode ser usada para fornecer detalhes adicionais sobre a árvore de menus e as funções que a usam.

   Clique em Salvar.

   A página Detalhes da árvore de menu para a nova árvore de menu é exibida.

5. Clique em Personalizar menu.

   Uma cópia da árvore de menu original é exibida.

6. Personalize a árvore do menu como desejado.

   Observação: para obter mais detalhes sobre adicionar, remover ou editar recursos da árvore de menu, consulte *Ajuda online*.

Criar e personalizar uma árvore de menu

É possível criar e personalizar árvores de menu com base em uma das árvores de menu padrão fornecidas.

Para criar e personalizar uma árvore de menu

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Árvores do menu na guia Administração.

   A página Lista de árvores de menus aparece.

2. Clique em Criar novo.

   A página Criar árvore de menus aparece.

3. Preencha os seguintes campos:

   Nome da árvore do menu

   (Obrigatório) O nome atribuído que identifica a árvore de menus.

   Código

   (Obrigatório) O código que identifica a árvore de menu para o sistema. Após definido, o código não pode ser alterado.

   Status do registro

   Indica se a árvore de menus está ativa ou inativa.

   Descrição

   Uma descrição da árvore de menus. A descrição pode ser usada para fornecer detalhes adicionais sobre a árvore de menus e as funções que a usam.

4. Clique em Salvar.

5. Clique em Personalizar menu.

   É exibido um formulário, permitindo a configuração da árvore de menu personalizada. Neste ponto, a árvore de menu contém somente um nó superior com o texto inserido como o nome da árvore de menu.

6. Clique com o botão direito do mouse na árvore de menu e selecione Criar novo nó.

   A página Criar nó aparece.

7. Preencha os seguintes campos:

   Nome do nó

   Insira o nome do nó. Esse é o nome exibido na árvore de menu.

   Descrição

   Insira uma descrição para o nó. A descrição pode ser usada para definir ainda mais a finalidade do nó.

   Recurso

   Insira o nome do recurso diretamente no campo ou clique no ícone de pesquisa para selecionar o recurso em uma lista. O recurso de árvore de menu determina a ação a realizar quando o usuário seleciona o nó na árvore de menu.

8. Repita as etapas 6 e 7 tantas vezes quantas forem necessárias para criar o conjunto de nós que deseja que sejam exibidos na árvore de menu.

   Observação: para obter mais informações sobre adicionar, remover ou editar recursos da árvore de menu, consulte a *Ajuda online*.

9. Clique em Salvar.

   A definição da árvore de menus é salva e a página Detalhes da árvore de menu aparece.

Criar e publicar um pacote de ajuda

Você pode criar conjuntos de ajuda personalizados para quaisquer funções que possa definir.

Para criar, preencher e publicar um pacote de ajuda

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Pacotes de ajuda na guia Administração.

   A página Lista de pacotes de ajuda aparece.

2. Clique em Criar novo.

   A página Criar pacote de ajuda aparece.

3. Preencha os seguintes campos:

   Nome do pacote da ajuda

   O nome exclusivo desse pacote de ajuda.

   Tipo de interface

   O tipo de interface do pacote de ajuda (como Analista, Funcionário ou Cliente).

   Status do registro

   Indica se o pacote de ajuda está ativo ou inativo.

Prefixo de nome de arquivo

O prefixo que você quer vincular aos arquivos de ajuda gerados para esse pacote de ajuda. Não inclua espaços no nome.

Observação: atribuir um prefixo que permite identificar os arquivos pertencentes a esse pacote de ajuda. Por exemplo, você pode usar ANA como o prefixo do pacote de ajuda do analista.

Interno

Isso é definido automaticamente como NÃO para conjuntos de ajuda definidos pelo usuário. Não é possível alterar o valor neste campo.

4. Clique em Salvar.

   A guia Conteúdo aparece.

5. Clique em Definir conteúdo.

   A janela Atualização de ajuda selecionada se abre.

6. Selecione o conteúdo que você deseja incluir no pacote de ajuda.

   Importante: Alguns tópicos são obrigatórios e são incluídos em seu novo pacote de ajuda, independentemente de você selecioná-los. Por exemplo, os tópicos da página inicial e outros assuntos preliminares do CA SDM são sempre incluídos. Da mesma forma, tópicos aninhados dependem dos tópicos que os contêm. Os tópicos que contêm outros serão automaticamente incluídos se você incluir um dos tópicos aninhados. Por exemplo, se selecionar o tópico "Usar o Gerenciador de filas", o tópico aninhado "Navegar CA SDM" é incluído ao publicar o pacote de ajuda.

7. Clique em OK.

   A janela Atualização de ajuda selecionada se fecha e o conteúdo é listado na guia Conteúdo.

8. Clique em Publicar.

   Isso gera o pacote de ajuda com o agrupamento dos tópicos selecionados em um sistema de ajuda que você pode exibir em um navegador da web.

9. Espere alguns momentos para o processo de publicação ser concluído e, em seguida, selecione Exibição, Atualizar na barra de menus.

   O botão Exibir ajuda fica ativo.

10. Clique em Exibir a ajuda.

    Seu pacote de ajuda personalizado aparece no navegador web padrão.

Alternar funções

Qualquer usuário com diversas funções atribuídas pode alternar entre funções sem efetuar logoff e voltar ao sistema. As funções são atribuídas aos usuários no Tipo de acesso ou registro de contato.

Observação: para obter mais informações, consulte Configurando contas de usuários (na página 215).

Para alternar funções

1. Selecione a função desejada na lista suspensa Função no canto superior direito da página principal do CA SDM.
2. Clique em Definir função

   A interface da web e as funcionalidades disponíveis para o usuário que efetuou logon para que correspondam à função atual.

Capítulo 7: Estabelecendo estrutura de suporte

Esta seção contém os seguintes tópicos:

Estrutura de suporte (na página 289)
Modelos (na página 290)
CA Workflow (na página 293)
Integração do fluxo de trabalho do CA Process Automation (na página 297)
Códigos compartilhados (na página 304)
Códigos de status (na página 307)
Tipos de tarefa (na página 313)
Acompanhamento de incidente (na página 314)
Solicitação/Incidente/Áreas de problemas (na página 316)
Categorias requisições de mudança e ocorrência (na página 321)
Fechamento automático de tickets (na página 327)
Atividades de ticket relacionadas (na página 329)
Cálculo de prioridade (na página 332)
Transições de status e controles de atributos dependentes (na página 351)
Transições de status para autoatendimento (na página 362)
Timers (na página 367)
Fusos horários (na página 368)
Anexos de arquivo (na página 371)
Anúncios (na página 376)
Configuração de consultas armazenadas (na página 377)
Números de sequência (na página 379)
Uso do log de auditoria (na página 380)
Integração com o CA Network and Systems Management (na página 380)

Estrutura de suporte

A *estrutura de suporte* de sua central de serviços consiste nos componentes necessários ao usuário a fim de resolver problemas. Você pode configurar a estrutura de suporte do CA SDM para que corresponda ao seu modelo de suporte (interno, externo ou ambos).

Observação: você pode personalizar ocorrências, solicitações e requisições de mudança para melhor atender às necessidades de seu local. Para obter mais informações, consulte o *Guia de Implementação* e a *Ajuda online*.

Modelos

O CA SDM oferece suporte aos seguintes modelos de service desk:

- Modelo interno
- Modelo externo
- Modelo combinado

Observação: para obter detalhes sobre como usar a interface da web para implementar seu modelo selecionado, consulte a *Ajuda online*.

Modelo interno

Um service desk interno dá suporte a funcionários que trabalham na empresa e que têm perguntas ou encontram problemas ao usar produtos e serviços fornecidos a eles pela empresa. No CA SDM, a solicitação é a unidade básica de suporte na operação de um service desk interno, como mostrado a seguir:

- Solicitações são tickets que manipulam as perguntas ou problemas de funcionários, e destinam-se a oferecer suporte à infra-estrutura possuída e administrada pela organização de suporte.
- Requisições de mudança são tickets que administram mudanças à infra-estrutura comercial suportada. Os service desks internos geralmente usam solicitações como o ticket primário, anexando requisições de mudança em casos em que a solicitação deve resultar em uma mudança à infra-estrutura.

Se você estiver operando um service desk interno, faça o seguinte:

- Analise os tipos de acesso de funcionários que usam a função administrativa da interface da web para ver se atendem às suas necessidades. Se a maioria de seus contatos for funcionários que usam o service desk para obter suporte, convém definir como "funcionário" o tipo de acesso padrão. Desse modo você não terá de definir o tipo de acesso para cada contato de funcionário que recebe suporte de seu service desk.
- Analise o tipo de contato de funcionário que usa a função administrativa da interface da web para ver se atende às suas necessidades.
- Certifique-se de que seus contatos estejam definidos usando o tipo de acesso e o tipo de contato apropriados. Por exemplo, se você definir funcionário como o tipo de acesso padrão, terá de definir os contatos de analista com o tipo de acesso de analista.

O tipo de contato normalmente é atribuído automaticamente com base em como você cria o contato, mas em alguns casos, o tipo de contato pode não estar definido. Os funcionários usando o service desk para obter suporte devem ter um tipo de contato de funcionário, ao passo que funcionários que trabalham como analistas de suporte devem ter um tipo de contato de analista.

Você pode trabalhar com contados usando a função administrativa da interface da web.

Se você estiver operando um service desk interno em que dá suporte a funcionários, sua estrutura de suporte consistirá em solicitações e requisições de mudança que eles criarem e nos recursos de suporte subjacentes a essas solicitações e requisições de mudança. Como administrador, você configura a estrutura de suporte.

Modelo externo

Um service desk externo dá suporte a clientes que compram produtos ou serviços de sua empresa e têm perguntas ou encontram problemas com esses produtos ou serviços. No CA SDM, a ocorrência é a unidade básica de suporte ao operar uma central de serviços externa. As ocorrências são tickets projetados para lidar com perguntas ou problemas de cliente, e têm como objetivo dar suporte a produtos e serviços adquiridos pelo cliente.

Se você estiver operando uma central de serviços externa:

- Analise o tipo de acesso de cliente que usa a função administrativa da interface da web para ver se atende às suas necessidades. Se a maioria de seus contatos são clientes, você talvez queira definir "cliente" como o tipo de acesso padrão.
- Analise o tipo de contato do cliente que usa a função administrativa da interface da web para ver se atende às suas necessidades.
- Certifique-se de que seus contatos estejam definidos usando o tipo de acesso e o tipo de contato apropriados. Por exemplo, se você definir cliente como o tipo de acesso padrão, terá de definir os contatos de analista com o tipo de acesso de analista.

O tipo de contato normalmente é atribuído automaticamente com base em como você cria o contato, mas em alguns casos, o tipo de contato pode não estar definido. Os clientes usando o service desk para obter suporte devem ter um tipo de contato de cliente, ao passo que os analistas que operam o service desk devem ter um tipo de contato de analista.

Você pode trabalhar com contados usando a função administrativa da interface da web.

Se você estiver operando um service desk externo em que dá suporte a clientes, sua estrutura de suporte consistirá em ocorrências que eles criarem e em recursos de suporte subjacentes a essas ocorrências. Como o administrador, você precisa configurar a estrutura de suporte usando as informações no restante deste capítulo. Cada tópico estabelece se as informações aplicam-se a seu modelo.

Modelo combinado

Algumas empresas precisam operar modelos tanto internos como externos de service desk. Neste caso, você pode agir de uma das seguintes maneiras:

- Separe modelos de service desk internos e externos com instalações distintas do service desk.
- Configure o CA SDM para suportar ambos os modelos.

  Essa configuração é conveniente quando seus analistas do service desk são treinados para dar suporte tanto a funcionários como a clientes, e quando a distinção entre suporte externo e interno não é sempre óbvia. Por exemplo, você pode ter funcionários que compram produtos de sua empresa ou clientes que têm problemas e perguntas relacionados à infraestrutura de sua empresa.

Como o administrador, você deve configurar a estrutura de suporte para um service desk interno/externo combinado, que consiste em ocorrências, solicitações e requisições de mudança, e suas características de suporte subjacentes. Se você decidir usar uma combinação de service desk interno e externo, faça o seguinte antes de configurar uma estrutura:

- Analise os tipos de acesso do cliente e do funcionário que usam a função administrativa da interface web para ver se atendem às suas necessidades. Se a maioria de seus contatos são clientes, você talvez queira definir "cliente" como o tipo de acesso padrão. Se a maioria de seus contatos for funcionários que usam o service desk para obter suporte, convém definir como "funcionário" o tipo de acesso padrão.

- Analise os tipos de contato do cliente e do funcionário que usam a função administrativa da interface web para ver se eles atendem às suas necessidades.
- Certifique-se de que seus contatos estejam definidos para ter o tipo de acesso e o tipo de contato apropriados. Por exemplo, se você definir cliente como o tipo de acesso padrão, terá que definir os contatos de analista com o tipo de acesso de analista e os contatos de funcionários com o tipo de acesso de funcionário.

  O tipo de contato normalmente é atribuído automaticamente com base no modo como você cria o contato como segue, mas, em alguns casos, o tipo de contato pode não estar definido.

  - Os clientes que usam seu service desk para suporte devem ter um tipo de contato de cliente.
  - Os funcionários que usam o service desk para suporte devem ter um tipo de contato de funcionário.
  - Os funcionários que trabalham como analistas de suporte devem ter um tipo de contato de analista.

  Você pode trabalhar com contados usando a função administrativa da interface web.

Mais informações:

Tipos de contato (na página 218)
Como funcionam os tipos de acesso (na página 254)

CA Workflow

Uma definição de processo do CA Workflow pode ser associada a qualquer tipo de ticket (na página 34) do CA SDM. A definição de processo que será aplicada a cada ticket é determinada pela categoria de mudança, categoria de ocorrência ou área de solicitação/incidente/problema a que o ticket é atribuído.

Se uma definição de processo do CA Workflow for associada com uma categoria ou área, quando um ticket é atribuído a essa categoria ou área, o CA Workflow cria uma instância de processo a partir da definição. O progresso da instância do processo é exibido na guia Tarefas do fluxo de trabalho do ticket.

É possível, opcionalmente, instalar o CA Workflow durante a instalação do CA SDM, ou você pode direcionar o CA SDM para usar uma instância diferente do CA Workflow atualizando várias opções no Gerenciador de opções, incluindo:

CAWF_USERNAME

Especifica o usuário do CA EEM com acesso total (concedido aos recursos "IDE" e "Processo") ao CA Workflow.

CAWF_PASSWORD

Especifica a senha para o cawf_username.

CAWF_PM_LOCATION

Especifica o local: http://<server>:8090/pm/

CAWF_PM_URL

Especifica o URL:
http://<wf_hostname>:<wf_tomcat_port>/pm/services/pmService2

CAWF_WL_LOCATION

Especifica o local: http://<server>:8090/wl/

CAWF_WL_URL

Especifica o URL: http://<server>:8090/wl/services/wlServic

Essas opções especificam vários pontos de finalização para o CA Workflow. Na maioria dos casos, você simplesmente necessita atualizar o servidor e a porta para que correspondam ao local do CA Workflow.

Importante: A mudança do servidor do CA Workflow tornará inoperantes as categorias, áreas ou tickets existentes vinculados às definições de processo e instâncias de processo no antigo servidor.

Workflow em Tempo de execução

Quando um ticket é salvo com uma categoria ou área vinculada a uma definição de processo do CA Workflow, uma instância da definição é criada. O progresso da instância é exibido na guia Tarefas do fluxo de trabalho do ticket. Como o CA Workflow pode incluir ramificações, apenas itens de trabalho concluídos e pendentes são exibidos.

Cada item de trabalho concluído e pendente, bem como o status geral do fluxo de trabalho, são exibidos na guia Tarefas do fluxo de trabalho. Ao clicar no link Nome de atividade, é exibido o aplicativo da web Lista de trabalho do CA Workflow, que é usado para completar itens individuais de trabalho.

Os dados da guia Fluxo de trabalho são recuperados diretamente do servidor do CA Workflow. Se o servidor de CA Workflow estiver indisponível, uma mensagem de erro será exibida na guia.

Selecione uma definição de processo de fluxo de trabalho

Uma definição de processo do CA Workflow deve ter um atributo de sequência de caracteres chamado *usd_persid* que gera um link a uma categoria de mudança/ocorrência ou a uma área de solicitação/incidente/problema. Esse atributo deve ser marcado como um parâmetro de entrada. Quando o CA SDM inicia a instância do CA Workflow, ele define usd_persid como identificador exclusivo (persistent_id) do ticket. Esse usd_persid pode ser usado para fazer chamadas de serviço web do CA Workflow para o CA SDM.

Importante: As categorias de mudança e ocorrência podem usar o sistema de fluxo de trabalho interno (clássico) do CA SDM ou o aplicativo CA Workflow. Os dois não podem ser usados ao mesmo tempo. As áreas solicitação/incidente/problema podem usar somente o aplicativo CA Workflow. O sistema de fluxo de trabalho clássico interno não é suportado para tickets de solicitação, incidente ou problema.

Para selecionar uma definição de processo do CA Workflow

1. Selecione uma categoria de mudança ou ocorrência. Por exemplo, para selecionar uma categoria de mudança, selecione Service Desk, Requisições de mudança, Categorias na guia Administração.

   A página Lista de categorias de mudança aparece.

2. Clique no símbolo da categoria de mudança que deseja editar.

   A página Detalhes da categoria de mudança aparece.

3. Clique no botão Usar o CA Workflow na guia Fluxo de trabalho.

   Observação: se você continuar esse procedimento e salvar a categoria, qualquer fluxo de trabalho de estilo do CA SDM anexado à categoria será excluído.

   Uma página de seleção aparece, listando as definições de processo do CA Workflow disponíveis.

4. Selecione uma definição de processo do CA Workflow.

   A Categoria é preenchida com a seleção.

5. Clique em Salvar.

   A categoria é atualizada com a definição de processo selecionada.

6. (Opcional) Altere a definição de processo do CA Workflow vinculada editando a categoria e clicando no hiperlink de definição do CA Workflow

   A página de seleção de definição de processo aparece.

   Observação: as definições de processo do CA Workflow serão exibidas na página de seleção somente se a definição tiver uma sequência de caracteres atribuída chamada usd_persid. Quando a definição for iniciada, esse atributo será definido com o valor de persistent_id do ticket. A definição de processo do CA Workflow também pode incluir um parâmetro de entrada de sequência de caracteres chamado *rótulo*. Se um rótulo for definido, o CA SDM definirá seu valor como o número do ticket. O número do ticket é exibido na lista de trabalho do CA Workflow e ajuda a fornecer contexto para o item de trabalho.

Tarefas de fluxo de trabalho

Tarefas de fluxo de trabalho identificam as atividades que devem ser completadas em tickets associados com uma categoria ou área específica. Assim como com as propriedades e outros aspectos da categoria ou área, as tarefas são automaticamente adicionadas aos tickets quando a categoria é selecionada. Definir tarefas de fluxo de trabalho permite a você fazer o seguinte:

- Especificar e descrever o tipo de tarefa a ser realizada.
- Atribuir um número seqüencial a cada tarefa.
- Especificar o usuário que deverá realizar a tarefa.
- Rastrear o andamento da resolução de tarefas atribuindo estados específicos válidos para cada tarefa.

Quando o status de uma tarefa muda, é possível executar certos comportamentos. Os comportamentos permitem definir as tarefas ou processos específicos executados quando a tarefa de fluxo de trabalho alcança um estado específico. Por exemplo, ao definir comportamentos, você pode enviar uma notificação de email a um gerente específico quando uma tarefa de aprovação exibe o estado Pendente.

Observação: para obter mais informações sobre como criar tarefas do fluxo de trabalho e definir comportamentos para elas, consulte a *Ajuda online*.

Integração do fluxo de trabalho do CA Process Automation

CA Process Automation é um produto CA autônomo com recursos para a automação e acompanhamento de tarefas de administração de hardware e software em ambientes de TI corporativos. CA Process Automation automatiza tarefas e gerencia interações do usuário, tais como aprovações e notificações de conformidade e precisão dentro dos ambientes de produção.

Quando você integra o CA SDM e o CA Process Automation, você pode aproveitar os benefícios dos recursos do workflow do CA Process Automation dos pontos chave no CA SDM. Uma integração eficaz entre o CA SDM e o CA Process Automation requer que você entenda ambos os produtos.

Mais informações:

Componentes do CA Process Automation (na página 298)
Integração do CA Process Automation com CA SDM em tempo de execução (na página 299)
Como criar uma definição de processo (na página 300)
Criar um formulário de solicitação inicial (na página 301)
Anexar uma definição de processo do CA Process Automation (na página 303)

Componentes do CA Process Automation

O CA Process Automation oferece varias capacidades e estruturas que facilitam uma ampla variedade de atividades como parte do gerenciamento de processos do CA Process Automation. Para a integração com o CA SDM, no entanto, somente os seguintes componentes do CA Process Automation são críticos para a integração com o CA Process Automation:

- **Definição de processo —** identifica uma série coletiva de tarefas, etapas e condições estruturadas em uma ordem específica para serem iniciadas e concluídas por vários indivíduos ou partes. Este componente é o bloco central de todo o conteúdo do CA Process Automation.
- **Formulário de solicitação de início —** um objeto contendo informações descritivas para os usuários finais. O Formulário de solicitação de início apresenta uma definição de processo para usuários enquanto oculta os detalhes técnicos da definição do processo.
- **Palavras-chave —** uma lista de palavras ou frases predefinidas para anexar a Formulários de solicitação de início.
- **Biblioteca de automação —** uma área dentro do CA Process Automation que armazena e exibe Definições do processo e Formulários de solicitação de início.
- **Caminho da biblioteca ou Caminho de referência —** uma estrutura de pasta que organiza e descreve Definições do processo e Formulários de solicitação de início dentro da biblioteca de automação.
- **Sessão do processo —** uma entidade ativa que executa as regras definidas em uma definição do processo. A sessão do processo avança até que o estado de definição do processo esteja completo.
- **Mensagens de log da sessão do processo —** um registro configurável em execução que detalha o progresso das atividades da sessão do processo. Categorias de mensagem de log são úteis para a integração do CA SDM com o CA Process Automation.

Observação: o escopo das definições dos componentes do CA Process Automation é limitado ao uso dentro do CA SDM. Para obter informações sobre os componentes e capacidades do CA Process Automation, consulte a documentação do CA Process Automation.

Integração do CA Process Automation com CA SDM em tempo de execução

Quando você ativa a integração, o usuário do CA SDM experimenta o seguinte:

- Em uma nova Solicitação, Requisição de mudança ou Ocorrência, uma instância de processo do CA Process Automation inicia com base na área ou categoria do ticket. Informações de resumo são imediatamente exibidas na guia Tarefas do workflow.
- Quando uma Área de solicitação, Categoria de mudança ou Categoria de ocorrência muda, uma instância de processo do CA Process Automation anexa encerra e uma nova instância de processo inicia.
- Quando um usuário do CA SDM tenta fechar uma Solicitação, Requisição de mudança ou Ocorrência onde a instância de processo do CA Process Automation ainda não está concluída, o usuário não consegue fechar o ticket. Em vez disso, o usuário deve primeiro cancelar o ticket. O status Cancelar encerra a instância do processo do CA Process Automation antes que o ticket feche.
- Quando um usuário deseja entender o estado da instância do processo sem navegar para longe do ticket, ele pode clicar na guia Tarefas do workflow do ticket. A guia Tarefas do workflow mostra a data de início da instância do processo, a data final, o estado atual e a trilha de auditoria atual de mensagens indicando o caminho da instância do processo.
- Quando um usuário deseja ver o caminho atual da instância de processo relativa a todo o processo, o usuário seleciona o botão Exibir processos na guia Tarefas do workflow. O botão Exibir processos abre um instantâneo gráfico de toda a instância do processo e mostra o caminho atual.
- Quando um usuário deseja ver os formulários de solicitação de interação do CA Process Automation que estão aguardando por ação do usuário, ele pode selecionar qualquer entrada na guia Tarefas do workflow. A guia Tarefas do workflow contém uma trilha de auditoria de mensagens da instância do processo que aparecem na lista de tarefas do CA Process Automation.

Observação: quando um usuário seleciona o botão Exibir processo do CA SDM ou mensagens da instância do processo do CA Process Automation, o sistema solicita um nome de usuário e senha do CA Process Automation para uma única sessão de navegador. Após a solicitação inicial, o sistema não solicita ao usuário novamente até que o navegador do CA SDM feche.

Como criar uma definição de processo

Ao criar a definição do processo, preencha o CA Process Automation com conteúdo para aparecer no CA SDM. Você usa o criador de processo gráfico do CA Process Automation para criar, testar e devolver uma definição de processo. No CA SDM, também é possível criar macros para iniciar os processos do CA Process Automation.

Observação: para obter informações sobre criação de macros do CA Process Automation, consulte a *Ajuda online*.

Para criar uma definição de processo no CA Process Automation, faça o seguinte:

1. Efetue logon no cliente CA Process Automation como usuário administrativo.
2. Use o criador de processo gráfico do CA Process Automation para criar, testar e devolver uma definição de processo. Ao trabalhar com a definição do processo, use as instruções na documentação do usuário do CA Process Automation.

   Observação: se você falhar em devolver a definição de processo antes de tentar usá-la, o workflow não operará adequadamente no CA SDM.

   Os seguintes itens da definição do processo estão disponíveis no CA SDM:

   Nome do processo

   Aparece na página Área de solicitação, Categoria de mudança e Detalhes da ocorrência. O nome do processo também aparece na guia Tarefas de workflow de um ticket. O nome do processo descreve a definição do processo para o CA SDM para Analistas e outros usuários que gerenciam tickets.

   Caminho de referência do processo

   Aparece nas páginas Área de solicitação, Categoria de mudança e Detalhes da ocorrência. O Caminho de referência do processo também aparece na guia de Tarefas de workflow do ticket. O Caminho de referência do processo pode ser útil para descrever o objetivo do processo a usuários finais. Por exemplo, "/Processes/Approval" não é útil. Em vez disso, um caminho de referência como "/Office Supplies/Approvals/Over-200-USD" descreve o fluxo de trabalho para gerenciar requisições que ultrapassam US$ 200.

Mensagens de log do processo

Aparece na guia Tarefas de workflow de ticket do CA SDM. Por padrão, um registro de atividades é armazenado com a instância do processo. Mensagens de log do processo possuem a categoria Processo. Um criador de processo pode criar mensagens personalizadas para aparecerem na guia Tarefas de workflow de um ticket do CA SDM.

Observação: para obter informações sobre a configuração da opção caextwf_log_categories para gerenciar mensagens de log, consulte o *Guia de Implementação*.

Criar um formulário de solicitação inicial

Ao criar um Formulário de solicitação inicial, associe-o à definição de processo e o devolva. Você inclui as palavras-chave adequadas nas propriedades do Formulário de solicitação inicial. Se a palavra adequada estiver faltando nas propriedades do Formulário de solicitação inicial, o Formulário de solicitação inicial e sua definição de processo associada falham em aparecer no CA SDM.

Para criar um Formulário de solicitação inicial

1. Efetue logon no cliente CA Process Automation como usuário administrativo.
2. Abra a Biblioteca do CA Process Automation e navegue para o caminho Formulário de solicitação inicial.

   O Formulário de solicitação inicial aparece na seção direita da biblioteca do CA Process Automation.
3. Selecione o Formulário de solicitação inicial na lista.

   Um menu de atalho é exibido.
4. Selecione Propriedades.

   A página Library Object Properties aparece.
5. (Opcional) Clique na guia Geral e modifique a descrição do Formulário de solicitação inicial. Adicione uma descrição que identifique o uso adequado do Formulário de solicitação inicial e a Definição de processos associada para o Administrador do CA SDM.
6. Clique na guia Palavras-chave.

   A guia Palavras-chave está ativa.
7. Clique no ícone ab+.

   Uma linha é adicionada à lista vazia.

8. Clique na linha.

   Um cursor intermitente destaca a linha e indica que a linha está pronta para digitação.

9. Insira um dos seguintes valores associados a uma palavra-chave à área ou categoria de ticket adequada. Por exemplo, para disponibilizar um Formulário de solicitação inicial para uma área de solicitação do CA SDM, insira a palavra-chave.

Ticket	Use a Palavra-chave
área de solicitação	pcat
categoria de mudança	chgcat
Categoria da ocorrência	isscat

10. Adicionar uma linha à lista para cada palavra-chave aplicável. Por exemplo, para fazer o Formulário de solicitação inicial aparecer em ambas as áreas de solicitação e categorias de mudança, adicione uma linha para a palavra-chave chgcat e outra para a palavra-chave pcat.

11. Clique em OK.

    O CA Process Automation salva as palavras-chaves e a descrição e fecha o diálogo Library Object Properties.

12. Devolva a Formulário de solicitação inicial.

    Observação: se você falhar em devolver o Formulário de solicitação inicial, o formulário falha em ser exibido no CA SDM.

    As informações do Formulário de solicitação inicial do CA Process Automation aparecem na Lista de formulário de solicitação inicial do CA SDM. O administrador do CA SDM pode associar o Formulário de solicitação inicial do CA SDM à Definição de processo em uma página de Área de solicitação, Categoria de mudança ou Detalhes da categoria.

    Os seguintes itens do Formulário de solicitação inicial aparecem no CA SDM:

    Nome do Formulário de solicitação inicial

    Aparece nas páginas Área de solicitação, Categorias de mudança e lista de Categorias de ocorrência.

    Caminho de referência do Formulário de solicitação inicial

    Aparece nas páginas Área de solicitação, Categorias de mudança e lista de Categorias de ocorrência.

Descrição do Formulário de solicitação inicial

Aparece nas páginas Área de solicitação, Categorias de mudança e lista de Categorias de ocorrência. O texto nesse campo descreve como o Formulário de solicitação inicial é adequado para seleção em uma Área de solicitação, Categoria de mudança ou Categoria de ocorrência em particular.

Anexar uma definição de processo do CA Process Automation

Ao vincular uma definição de processo do CA Process Automation a uma área ou categoria de ticket do CA SDM, você cria uma conexão estática entre uma área ou categoria de ticket do CA SDM e uma definição de processo do CA Process Automation.

Quando um usuário do CA SDM cria ou edita um ticket e seleciona uma categoria de ticket, a definição de processo do CA Process Automation associada inicia em uma instância de processo. Informações pertinentes sobre a instância do processo aparecem na guia Tarefas do fluxo de trabalho no ticket.

Para vincular uma definição de processo

1. Na guia Administração, selecione Service Desk.
2. Navegue para as Áreas ou Categorias do ticket.

   A Lista de categoria ou área aparece.
3. Criar ou editar uma área ou categoria de ticket.

   A página Atualizar aparece.
4. Clique na guia Fluxo de trabalho.

   Se as Opções do CA Process Automation estiverem instaladas no Gerenciador de opções do CA SDM o botão Usar CA IT PAM está disponível na guia Workflow.
5. Clique em Usar CA IT PAM,

   A lista do Formulário de solicitação inicial do CA IT PAM aparece. Cada linha na lista é um Formulário de solicitação inicial do CA Process Automation.

   Observação: você pode usar o workflow interno do CA Process Automation, CA Workflow ou CA SDM para gerenciar diferentes áreas ou categorias de ticket. Entretanto, uma única categoria pode usar somente uma ferramenta de workflow por vez.

6. Clique no valor na coluna Nome para selecionar a definição de processo associada a esse Formulário de solicitação inicial.

   A lista do Formulário de solicitação inicial do CA IT PAM se fecha. O nome da definição de processo e o caminho de referência da definição de processo aparecem na guia Workflow.

7. Clique em Salvar.

   O sistema salva as configurações do processo. O próximo ticket que um usuário crie na área ou categoria de ticket especificada automaticamente vincula o workflow e cria uma instância de processo. A guia Tarefas do workflow do ticket mostra um resumo das informações da instância de processo. Além disso, o usuário pode acessar mais informações sobre a instância de processo clicando em Exibir processo na guia Tarefas do workflow.

Códigos compartilhados

No CA SDM, os tipos de tickets diferentes compartilham certos códigos subjacentes, como prioridade, gravidade, impacto e de urgência. As solicitações e requisições de mudança compartilham alguns códigos; e todos os tipos de tickets compartilham outros códigos.

Considere as seguintes informações sobre códigos compartilhados:

- Por padrão, valores numéricos classificam os códigos.
- Você pode personalizá-los.
- Você não pode adicionar nem excluir códigos compartilhados.
- Você pode usar códigos de impacto, prioridade, gravidade e de urgência.

De acordo com seu modelo de service desk, configure os seguintes códigos:

Códigos compartilhados	Descrição
Prioridade	Deve ser configurado para todos os modelos de service desk.
Gravidade	Deve ser configurado para os modelos de service desk interno e combinado.
Impacto	Deve ser configurado para os modelos de service desk interno e combinado.

Códigos compartilhados	Descrição
Urgência	Deve ser configurado para os modelos de service desk interno e combinado.

Observação: para obter detalhes sobre como personalizar esses códigos usando a função administrativa da interface web, consulte a *Ajuda online*.

Mais informações:

Códigos de prioridade (na página 305)
Códigos de gravidade (na página 306)
Códigos de impacto (na página 306)
Códigos de urgência (na página 306)

Códigos de prioridade

Os códigos de prioridade indicam a ordem de classificação segundo a qual o service desk deve responder aos tickets (isto é, especifica o nível de atenção que um ticket deve receber). Os códigos de prioridade são indicados em solicitações, requisições de mudança e ocorrências; portanto, aplicam-se a todos os modelos de service desk.

É possível usar prioridades para escalonar tickets manual ou automaticamente com a monitoração de eventos. Em muitas instalações de service desk, códigos de prioridade são usados no placar para fornecer aos analistas um status em tempo real de suas solicitações e requisições de mudança.

Você pode atribuir um tipo de serviço a um código de prioridade, e esse tipo será automaticamente atribuído a tickets quando o código de prioridade for especificado. Isso permite associar um nível específico de serviço a um ticket de acordo com a prioridade designada. Por exemplo, o tipo de serviço definido pelo sistema, resolução de 4 horas, é automaticamente associado com a prioridade 1. Tickets que tenham sido atribuídos uma prioridade de 1, portanto, têm automaticamente atribuídos este tipo de serviço, incluindo todos os eventos de tipo de serviço que estejam associados com o tipo de serviço de resolução de 4 horas.

Mais informações:

Contratos de nível de serviço (na página 170)
Como implementar tipos de serviço (na página 173)

Códigos de gravidade

Os códigos de gravidade identificam a extensão do dano ao equipamento afetado por uma solicitação. Os códigos de gravidade são indicados apenas em solicitações; portanto, aplicam-se somente a modelos combinados e internos de service desk.

Observação: a gravidade é geralmente usada como um sinônimo para prioridade. Alguns locais usam apenas códigos de prioridade, ignorando completamente a gravidade. Se quiser distinguir entre o nível de gravidade de um problema no âmbito técnico (gravidade) e quão rapidamente você quer lidar com ele (prioridade), use códigos de gravidade e de prioridade.

Os valores do código de impacto ajudam a calcular a prioridade do incidente.

Códigos de impacto

Os códigos de impacto estabelecem a importância de um ticket para a operação do sistema. Por exemplo, se uma requisição de mudança afetar o funcionamento do sistema inteiro, será atribuído um alto impacto a ele. Os códigos de impacto são indicados apenas em solicitações e requisições de mudança; portanto, aplicam-se somente a modelos combinados e internos de service desk.

Observação: os códigos de urgência (na página 306) e impacto são semelhantes, mas têm propósitos distintos.

Códigos de urgência

Os códigos de urgência medem a importância da solicitação para usuários do sistema (isso é, indicam a importância da solicitação ao ambiente total de produção). Por exemplo, se uma solicitação puder prejudicar a missão da empresa, o código de Urgência pode ter o valor 5-Imediato. Os códigos de urgência são indicados apenas em solicitações; portanto, aplicam-se somente a modelos combinados e internos de service desk.

Os códigos de urgência e impacto servem propósitos distintos, mas são freqüentemente confundidos porque coincidem. Por exemplo, uma solicitação para reportar um incêndio em um centro de dados crítico pode ter uma Urgência 3-Impacto de grupo único e 5-Imediato. Estes códigos aplicam-se porque o incêndio impacta mais do que um grupo, mas não necessariamente a organização inteira. Como o centro de dados é crítico para operações, a urgência requer atenção imediata.

Códigos de status

Os códigos de status são usados para monitorar o status de um item. Separe o rastreamento de códigos de status para solicitações, requisições de mudança, ocorrências e tarefas do fluxo de trabalho. Em cada caso, há códigos de status predefinidos que você pode usar para atender às suas necessidades. Do contrário, você pode modificar os códigos de status predefinidos ou definir novos que sejam específicos a sua organização. Dependendo de seu modelo de service desk, você configura os seguintes códigos:

Códigos de status	Descrição
Solicitação	Deve ser configurado para os modelos de service desk interno e combinado.
Requisição de mudança	Deve ser configurado para os modelos de service desk interno e combinado.
Ocorrência	Deve ser configurado para os modelos de service desk externo e combinado.
Tarefa	Deve ser configurado para todos os modelos de service desk.

Os códigos de status permitem aos analistas classificar e selecionar informações com base no status, de modo que possam monitorar de perto seu progresso. O cuidado tomado ao definir os códigos de status determina a precisão dos analistas ao descrever o status real de um item.

Você pode marcar qualquer código de status como ativo ou inativo. Quando marca um código de status como inativo, ele não fica mais disponível ao uso pelos analistas, mas permanece disponível para uso futuro (isso é, não é excluído do banco de dados). Se decidir mais tarde usar o código de status, você poderá marcá-lo como ativo.

Observação: as mesmas definições de área estão disponíveis para tickets de solicitação, incidente e problema. Na guia Administração, estas áreas são referenciadas como áreas de solicitação/incidente/problema. Por motivo de brevidade, elas são aqui denominadas simplesmente como áreas de solicitação.

Códigos de status de solicitação

A tabela a seguir descreve os códigos de status predefinidos para tickets de solicitação.

Código de status de solicitação	Descrição
Confirmada	O recebimento de uma solicitação foi reconhecido.
Fechado	Uma solicitação foi completamente resolvida.
Fechado — Sem resolver	Uma solicitação foi fechada mas ainda precisa ser resolvida.
Correção em andamento	Uma solicitação está aguardando a resolução.
Em espera	Os eventos de tipo de serviço da solicitação estão temporariamente suspensos.
Abrir	Uma solicitação foi definida e está sendo usada para controlar e administrar sua conclusão.
Problema fechado	Uma solicitação de problema foi completamente fechada.
Problema corrigido	Uma solicitação de problema foi resolvida, mas não foi fechada.
Problema aberto	Uma solicitação foi identificada como um problema.
Pesquisando	Uma solicitação está aberta e exige pesquisa e análise adicionais.
Trabalho em andamento	O trabalho está sendo feito para corrigir uma solicitação.

Se sua localidade usar outra terminologia para identificar o status de uma solicitação, você deve definir códigos de status que atendam às suas necessidades e ignorar os códigos de status predefinidos, ou alterar as definições para que elas atendam às suas necessidades. Por exemplo, você pode definir códigos de status de solicitação adicionais, como os seguintes:

Código de status de solicitação	Descrição
Duplicada	Uma solicitação foi aberta, mas pode ser uma cópia de uma solicitação existente de outro usuário.
Emergência	Solicitações importantes que devem receber atenção imediata.
Relatório	Solicitações que foram resolvidas e fechadas, mas que devem ser relatadas a um nível da gerência.
Teste	Solicitações que foram resolvidas, mas que devem ser testadas durante uma semana antes de serem fechadas.

Códigos de status de requisição de mudança

A tabela a seguir descreve os códigos de status predefinidos para tickets de requisição de mudança.

Código de status da requisição de mudança	Descrição
Aprovação em andamento	Uma requisição de mudança está aberta, com aprovação pendente.
Aprovado	Uma requisição de mudança foi aprovada.
Cancelado	Uma requisição de mudança foi cancelada.
Fechado	Uma requisição de mudança foi concluída.
Em espera	Os eventos de tipo de serviço da requisição de mudança estão temporariamente suspensos.
Implementação em andamento	Uma requisição de mudança está sendo implementada.

Código de status da requisição de mudança	Descrição
Abrir	Uma requisição de serviço foi definida em uma requisição de mudança, e a requisição de mudança está sendo usada para controlar e administrar sua conclusão.
Rejeitado	Uma requisição de mudança foi rejeitada.
Resolvido	Uma requisição de mudança foi resolvida.
RFC	Uma solicitação de mudança foi enviada.
Suspenso	Interrompe tarefas de fluxo de trabalho em uma requisição de mudança.
Verificação em andamento	Uma requisição de mudança está sendo verificada.
Recuar	A requisição de mudança implementada foi retirada.
Implementado	A mudança foi implementada.

Se sua organização usa outra terminologia para identificar o status de uma requisição de mudança, você deve definir códigos de status que atendam às suas necessidades e ignorar os códigos de status predefinidos, ou alterar as definições para que correspondam ao que necessita. Por exemplo, você pode definir códigos de status de uma requisição de mudança adicionais, como os listados na tabela a seguir:

Código de status de solicitação personalizado	Descrição
Duplicada	As requisições de mudança que foram abertas, mas podem ser uma duplicação de uma requisição de mudança existente para outro usuário.
Emergência	Requisições de mudança importantes que devem receber atenção imediata.
Relatório	Requisições de mudança que foram resolvidas e fechadas, mas que devem ser relatadas a um nível da gerência.

Códigos de fechamento

Use códigos de fechamento para definir o resultado final de requisições de mudança, como bem-sucedido ou sem êxito. Defina os códigos de fechamento manualmente ou como parte da atividade de atualização de status em uma requisição de mudança quando o status for fechado, concluído ou resolvido.

Observação: para obter mais informações sobre como criar ou definir códigos de fechamento e detalhes sobre as opções *require_closure_code* e *force_closure_code*, consulte a *Ajuda online*.

Códigos de status da ocorrência

A tabela a seguir descreve os códigos de status predefinidos para tickets de ocorrência.

Código de status de ocorrência	Descrição
Aprovação em Andamento	Uma ocorrência está aberta, com aprovação pendente.
Cancelado	Uma ocorrência foi cancelada.
Fechado	Uma ocorrência foi concluída.
Em espera	Os eventos de tipo de serviço da ocorrência estão temporariamente suspensos.
Implementação em andamento	Uma ocorrência está sendo implementada.
Abrir	Uma ocorrência foi definida e aberta, de modo que pode ser controlada e administrada até ser resolvida.
Suspenso	Interrompe tarefas de fluxo de trabalho em uma ocorrência.
Transação em andamento	Uma transação com um cliente relacionada a essa ocorrência está em andamento.
Verificação em Andamento	Uma ocorrência está sendo verificada.

Se sua organização usa outra terminologia para identificar o status de uma ocorrência, você deve definir códigos de status que atendam às suas necessidades e ignorar os códigos de status predefinidos, ou alterar as definições para que correspondam ao que necessita. Por exemplo, você pode definir códigos de status de ocorrência adicionais, como:

Código de status de ocorrência personalizado	Descrição
Duplicada	Uma ocorrência foi aberta, mas pode ser uma cópia de uma ocorrência existente de outro usuário.
Emergência	Ocorrências importantes que devem receber atenção imediata.
Relatório	Ocorrências que foram resolvidas e fechadas, mas que devem ser relatadas a um nível da gerência.

Códigos de status da tarefa

Os códigos de status da tarefa descrevem os possíveis estados diferentes de uma tarefa de fluxo de trabalho. Cada tarefa em um fluxo de trabalho de ocorrência ou requisição de mudança tem seu próprio status, separado do status do ticket. As tarefas de fluxo de trabalho permitem aos analistas acompanhar o tempo de conclusão de tarefas individuais em um ticket.

A tabela a seguir descreve os códigos de status predefinidos para tarefas de fluxo de trabalho.

Código de status da tarefa	Descrição
Aprovar	Tarefa aprovada.
Cancelado	A tarefa foi cancelada e não é possível atualizá-la.
Concluído	A tarefa foi concluída.
pendente	A tarefa foi iniciada.
Rejeitar	A tarefa foi rejeitada.
Reabrir	A tarefa foi- reaberta.
Reabrir–Aguardar	Uma tarefa prévia foi reaberta.
Ignorar	A tarefa é ignorada.

Código de status da tarefa	Descrição
Aguardar	A tarefa não foi iniciada.

Se sua organização usa outra terminologia para identificar o status de um fluxo de trabalho, você deve definir códigos de status que atendam às suas necessidades e ignorar os códigos de status predefinidos, ou alterar as definições para que correspondam ao que necessita.

Para cada código de status da tarefa, você pode atribuir um tipo de comportamento que ocorre quando a tarefa alcança esse estado, o que fornece muito mais informações sobre o andamento da conclusão da tarefa. Você também pode usar a função acumular para monitorar o tempo e o custo envolvidos na conclusão do ticket.

Tipos de tarefa

Os tipos de tarefa ajudam a determinar o comportamento das tarefas de fluxo de trabalho específicas e os códigos de status da tarefa. Para produzir características que definam cada tipo de tarefa, você pode identificar os códigos de status da tarefa ou estados específicos que podem ser usados.

Como tanto requisições de mudança quanto ocorrências usam tarefas de fluxo de trabalho, defina os tipos de tarefa para todos os modelos de service desk. Os códigos de status da tarefa identificam os comportamentos associados a cada tarefa. Por exemplo, você pode configurar o tipo de tarefa Aprovação para permitir os estados Aprovar, Rejeitar, Pendente e Aguardar como estados disponíveis. Quando o tipo de tarefa Aprovação entrar no estado Pendente, você poderá enviar notificação a um gerente ou analista específico e assim por diante.

Você pode marcar qualquer tipo de tarefa como ativo ou inativo. Quando você marca um tipo de tarefa como inativo, ele não pode mais ser usado por analistas, mas permanece disponível para uso futuro (não é excluído do banco de dados). Se, posteriormente, você decidir usar o tipo de tarefa, marque-o novamente como ativo.

Observação: você pode exibir os tipos de tarefa predefinidos na página Lista de tipos de tarefa da função administrativa da interface da web.

Exemplo: códigos de status da tarefa

A tabela a seguir contém alguns exemplos de códigos de status:

Código de status da tarefa	Descrição
Aprovação	Aprovar ou rejeitar ticket
Tarefa final de grupo	Término das tarefas do grupo
Tarefa inicial de grupo	Início das tarefas do grupo
Iniciar aprovação	Aprovação para iniciar o ticket

Neste exemplo, os tipos Tarefa inicial de grupo e Tarefa final de grupo definem um grupo de tarefas em uma ocorrência ou categoria de mudança que precisam ser realizadas. As tarefas no grupo podem ser executadas em qualquer requisição. Depois que a tarefa inicial de grupo está no estado Pendente (iniciada), todas as tarefas do grupo também são colocadas nesse estado.

Observação: para obter mais informações sobre o uso de tipos de tarefas, consulte a *Ajuda online*.

Acompanhamento de incidente

O acompanhamento de incidente permite que os analistas acompanhem um incidente selecionando um ou mais sinalizadores para o incidente. As informações que os analistas especificam fornecem a sua organização métricas sobre incidentes para relatórios. Por exemplo, os analistas podem indicar que um incidente foi atribuído incorretamente. Quando é exibida em um relatório uma grande porcentagem de tickets atribuídos incorretamente, sua organização está ciente de que as atribuições devem ser corrigidas.

Por exemplo, os analistas podem especificar informações para ajudar sua organização a fazer o seguinte:

- Melhorar a responsividade do SLA e fechamento em níveis inferiores dentro da organização de suporte.

- Identificar tickets que estão incorretamente atribuídos.
- Indicar que foi usada uma ferramenta de controle remoto para resolver ticket.

Você instala a opção efficiency_tracking do Gerenciador de opções para que analistas possam usar opções de acompanhamento que aparecem na guia Acompanhamento de eficiência das páginas de detalhes do incidente.

Observação: para obter mais informações sobre o acompanhamento de incidentes, consulte a *Ajuda online*.

Instalar acompanhamento de incidente

É possível instalar uma opção para permitir que os analistas acompanhem um incidente configurando sinalizadores particulares para o incidente. As informações que os analistas especificam fornecem a sua organização métricas sobre incidentes para relatórios. Após instalar a opção, o sinalizador de acompanhamento aparece na guia Acompanhamento de eficiência das páginas de detalhes do incidente.

Para instalar o acompanhamento de incidentes

1. Na guia Administração, navegue para Gerenciador de opções, Gerenciador de solicitações.

   A Lista de opções aparece.

2. Clique em efficiency_tracking.

   A página Detalhes de opções efficiency_tracking aparece com os valores padrão definidos.

3. Clique em Editar.

   A página Atualizar opções efficiency_tracking aparece com os valores padrão definidos e você pode editar a Descrição.

4. Clique em Instalar.

   A página Detalhes de opções efficiency_tracking aparece.

5. Clique em Fechar janela.

   O acompanhamento de incidente é instalado; entretanto, a guia Acompanhamento de eficiência não aparece nas páginas de detalhes do incidente.

6. Reinicialize o CA SDM.

   A guia Acompanhamento de eficiência aparece nas páginas de detalhes do incidente.

Solicitação/Incidente/Áreas de problemas

As áreas de solicitação definem os grupos lógicos em que os tickets de solicitação, incidente e problema podem ser organizados. Por exemplo, tickets relacionados a um aplicativo podem ser atribuídos a uma área predefinida de Aplicativos. Sempre que um analista atribui um ticket a uma área de solicitação, todas as informações associadas à área são automaticamente inseridas no ticket. Por exemplo, se você indicar um tipo de serviço, ele será associado ao ticket e todos os seus eventos de tipo de serviço associados.

Observação: as mesmas definições de área estão disponíveis para tickets de solicitação, incidente e problema. Na guia Administração da interface da Web do CA SDM, estas áreas são referenciadas como áreas de solicitação/incidente/problema. Por motivo de brevidade, elas são aqui denominadas simplesmente como áreas de solicitação.

É possível definir qualquer área de solicitação como ativa ou inativa. Ao tornar uma área de solicitação inativa, ela não estará mais disponível para que analistas a usem, mas ela não é excluída do banco de dados. Se decidir posteriormente usar a área de solicitação, é preciso somente modificar o status novamente como ativo.

Você pode usar áreas de solicitação para fazer o seguir:

- Especificar valores padrão para os campos de grupo e responsável nos tickets.
- Associar automaticamente um nível de serviço aos tickets, atribuindo um tipo de serviço padrão à área de solicitação.
- Associar uma pesquisa a uma área de solicitação.
- Selecionar e gerar relatórios sobre tickets por área, definindo suas próprias áreas de solicitação personalizadas. Eventualmente, estudar tendências de solicitação e analisar causas de problemas. Concentrar sua observação em áreas de solicitação específicas pode tornar esses estudos ainda significativos e relevantes.

As seguintes áreas de solicitação predefinidas são instaladas com o CA SDM:

- Aplicativos
- Email
- Hardware
- Redes
- Impressora
- Software

  A área Software é subdividida em várias áreas de solicitação diferentes.

Observação: para obter informações sobre definição e edição de áreas de solicitação, consulte a *Ajuda online*.

Mais informações:

Propriedades de Área de solicitação/incidente/problema (na página 318)
Definir áreas de solicitação/incidente/problema para autoatendimento (na página 320)

Propriedades de Área de solicitação/incidente/problema

Você pode usar as propriedades para adicionar qualidades ou atributos personalizados a uma área de solicitação específica. Se você adicionou propriedades a uma área de solicitação, quando um analista atribuir um ticket àquela área as propriedades associadas aparecerão automaticamente na guia Propriedades do ticket. Por exemplo, você pode adicionar propriedades por email à área de solicitação predefinida para especificar o servidor de email ou o tamanho da caixa de correio.

Na medida em que se define propriedades, é possível especificar se um valor é obrigatório ou opcional. Para propriedades com um valor obrigatório (na página 318), os usuários deverão inserir um valor (ou aceitar o padrão) para salvar o ticket.

A opção keep_tasks determina o que acontece quando você atribui um ticket existente a uma área de solicitação diferente:

- Se keep_tasks não estiver instalado, as propriedades existentes (bem como as tarefas do fluxo de trabalho) serão removidas do ticket e todas as propriedades ou tarefas associadas à nova área de solicitação serão adicionadas a ele.
- Se keep_tasks estiver instalado, as propriedades e tarefas existentes serão retidas no ticket e todas as propriedades ou tarefas associadas à nova área de solicitação serão adicionadas.

Observação: para obter instruções detalhadas sobre como adicionar propriedades a uma área de solicitação e como definir regras de validação de propriedade, consulte a *Ajuda online*.

Regras de validação da propriedade

É possível definir regras de validação para restringir os valores de propriedade que os usuários podem inserir para um conjunto predefinido de valores selecionáveis. Por exemplo, se você definiu uma propriedade chamada Sistema operacional, poderá definir a regra de validação como uma lista suspensa contendo as opções Windows, UNIX e Linux.

Propriedades definidas sem regras de validação são apresentadas ao usuário como caixas de texto livre, que permitem que qualquer sequência de caracteres seja informada. As regras de validação podem tornar a elaboração de relatórios sobre valores de área e categoria menos complexa e propensa a erros.

Observação: as regras de validação de propriedade são reutilizáveis. Elas não são específicas para uma propriedade em particular. É possível aplicar qualquer regra de validação existente a propriedades definidas para categorias de mudança, categorias de ocorrência ou áreas de solicitação/incidente/problema.

Dependendo do tipo de regra de validação que você configurou para uma propriedade, quando o usuário atribuir um ticket à categoria ou área a que essa propriedade está anexada, um dos seguintes controles é exibido na guia de propriedades do ticket:

- Text Edit Box—nenhuma regra de validação foi definida e nenhum valor padrão pode ser especificado. Espera-se que os usuários insiram valores que sigam os exemplos fornecidos por você.
- Check Box—uma caixa de seleção de dois estados é exibida na guia Propriedades. Por padrão, a caixa de seleção não está marcada. O usuário pode aceitar o padrão ou marcar a caixa de seleção. As caixas marcadas são exibidas na página de detalhes do ticket com Sim na coluna Valor. Caixas desmarcadas são exibidas com um Não na coluna de valor.
- Drop-down List—uma lista suspensa contendo um conjunto predefinido de opções é exibida na guia Propriedades. Se você tiver definido um valor padrão, ele será selecionado quando a lista suspensa for exibida pela primeira vez. A opção que o usuário seleciona é mostrada na coluna Valor da página de detalhes do ticket.

Definir áreas de solicitação/incidente/problema para autoatendimento

A opção Inclusão de autoatendimento permite definir quais áreas de solicitação/incidente/problema devem ser incluídas nos tickets para autoatendimento. Também é possível definir diferentes símbolos de autoatendimento em comparação àqueles vistos pelo analista. Quando o ticket é salvo, o símbolo de autoatendimento é exibido no campo da Área de solicitação/incidente/problema. Se o ticket é exibido na interface do analista, o símbolo normal para a área é exibido. O usuário do autoatendimento não tem permissão para editar o símbolo; ele é somente leitura.

Para definir uma área de solicitação/incidente/problema para autoatendimento

1. Na guia Administração, selecione Service Desk, Solicitações/incidentes/problemas, Áreas.

   A lista Área de solicitações/incidentes/problemas é exibida:

2. Selecione Editar na lista.

   A parte superior da página exibe os campos editáveis.

3. Abra a área de incidente/problema/solicitação desejada para editar na lista Símbolo (Hardware.pc.instalação, por exemplo).

4. Preencha os seguintes campos:

   Inclusão de autoatendimento

   Especifica se a área solicitação/incidente/problema é mostrada na interface de autoatendimento.

   Símbolo de autoatendimento

   Especifica um identificador único para essa área de solicitação/incidente/problema na interface de autoatendimento.

   Ativo

   Especifica onde a área de solicitação/incidente/problema está ativa ou inativa.

   A área solicitação/incidente/problema é definida para autoatendimento.

5. Clique em Salvar.

   A área de solicitação/incidente/problema atualizada aparece na Lista de áreas de solicitação/incidente/problema quando a lista é exibida novamente.

Categorias requisições de mudança e ocorrência

Categorias de mudança e categorias de ocorrência definem os agrupamentos lógicos nos quais requisições de mudança e ocorrências podem ser organizadas.

Observação: ao contrário das áreas de solicitação/incidente/problema, as categorias de requisição de mudança e as categorias de ocorrência são gerenciadas separadamente:

- Configure categorias de mudança para os modelos combinados e internos do CA SDM.
- Configure categorias de ocorrências para os modelos combinados e externos do CA SDM.

Você pode usar categorias para especificar valores padrão para certos campos em tickets. Você pode associar automaticamente um nível de serviço ao ticket ao atribuir um tipo de serviço padrão a categorias. Você também pode associar uma pesquisa a uma categoria.

Para cada categoria, você pode definir propriedades ou qualidades a serem associadas ao ticket e criar um fluxo de trabalho que identifique todas as tarefas individuais necessárias para concluir o ticket. Ao definir comportamentos associados às tarefas de fluxo de trabalho, você poderá notificar pessoas-chave quando o status da tarefa mudar ou quando atividades forem executadas para fechar o ticket.

Sempre que um analista atribui um ticket a uma categoria, todas as informações associadas à categoria são automaticamente inseridas no ticket. Por exemplo, se você indicar um tipo de serviço, ele será associado ao ticket e a seus eventos de tipo de serviço associados.

Observação: para obter informações sobre definição e edição de categorias, consulte a *Ajuda online*.

Mais informações:

Categorias de mudança predefinidas (na página 322)
Categorias de ocorrência predefinidas (na página 322)
Regras para alterar categorias em um ticket (na página 322)
Propriedades de categorias (na página 323)
Defina as categorias de mudança e ocorrência para um autoatendimento (na página 326)

Categorias de mudança predefinidas

Os seguintes conjuntos de categorias de mudança predefinidas são instalados com o CA SDM:

- Adicionar
- Mudança
- Mover
- Desativar

Observação: todos esses conjuntos de categorias são subdivididos em categorias mais específicas. Por exemplo, a Categoria de mudança definida inclui categorias para alterar servidores e estações de trabalho.

Categorias de ocorrência predefinidas

As seguintes categorias de ocorrência predefinidas são instaladas com o CA SDM:

- Hardware.pc.instalação
- Software.pc.instalação

É possível configurar o status de qualquer categoria como ativo ou inativo. Ao tornar uma categoria inativa, ela não está mais disponível para uso dos analistas, mas não foi excluída do banco de dados. Se mais tarde decidir usar a categoria, retorne o status para ativo.

Regras para alterar categorias em um ticket

As seguintes regras afetam apenas as tarefas de fluxo de trabalho.

- Se a categoria anterior usava o CA Workflow ou o Classic Workflow e a nova categoria usa o CA Process Automation, a definição do processo do CA Process Automation possui uma vinculação para um fluxo de trabalho em um servidor CA Process Automation.
- Se tanto a nova categoria quanto a antiga usar o fluxo de trabalho do CA SDM, as regras das versões anteriores serão válidas.

- Se a nova categoria usa o CA Workflow ou CA Process Automation e a anterior usa o fluxo de trabalho do CA SDM, ocorre o seguinte:
  - Todas as tarefas de fluxo de trabalho incompletas e pendentes (tarefas que podem ser atualizadas) com o estilo do CA SDM 6.0 são definidas com o status Cancelado, independentemente da opção KEEP_TASKS. Quaisquer tarefas concluídas do fluxo de trabalho permanecem, mas não podem ser reabertas.
  - Todas as tarefas não ativas e incompletas (como as tarefas com o status Aguardar) são excluídas.
  - A definição do CA Workflow ou CA Process Automation é instanciada.
- Se a nova categoria usa o fluxo de trabalho do CA SDM e a antiga usa o CA Workflow ou CA Process Automation, então ocorre o seguinte:
  - A instância do CA Workflow ou CA Process Automation é forçosamente definida para o status Encerrado.
  - As novas tarefas de fluxo de trabalho da categoria são adicionadas como normalmente.
- Se tanto a categoria antiga como a nova usam o CA Workflow, ocorre o seguinte:
  - Se as categorias nova e antiga apontam para a mesma definição de processo, a instância em execução da categoria anterior continua ativa.
  - Se as categorias nova e antiga apontam para definições de processo diferentes, a instância antiga é definida como Encerrado e a definição da nova categoria é instanciada.

Em um fluxo de trabalho do CA SDM, um ticket com uma instância do CA Workflow ou CA Process Automation em execução não pode ser fechado. As funções Acumular, Agilizar e Inserir tarefa estão desativadas para tickets que usam o CA Workflow.

Propriedades de categorias

Propriedades são usadas para adicionar atributos ou qualidades personalizados para uma categoria específica. Se você adicionou propriedades a uma categoria, quando um analista atribuir um ticket a essa categoria as propriedades associadas aparecerão automaticamente na guia Propriedades do ticket.

Por exemplo, você pode adicionar propriedades à categoria de ocorrência Software.pc.install para especificar o tamanho da memória, o tipo de processador, etc.

Na medida em que se definem propriedades, é possível especificar se um valor é obrigatório ou opcional. Para propriedades com um valor obrigatório, os usuários deverão inserir um valor (ou aceitar o padrão) para salvar o ticket.

Retenção de propriedades de categoria

A opção keep_tasks determina o que acontece se você atribuir um ticket existente a uma categoria diferente:

- Se keep_tasks não estiver instalado, as propriedades existentes e as tarefas do fluxo de trabalho serão removidas do ticket, e todas as propriedades ou tarefas associadas à nova categoria serão adicionadas a ele.
- Se keep_tasks estiver instalado, as propriedades e tarefas existentes são retidas no ticket, e todas as propriedades ou tarefas associadas à nova categoria são adicionadas.

Observação: para obter instruções detalhadas sobre como adicionar propriedades a uma categoria de mudança ou de ocorrência e como definir regras de validação de propriedade, consulte a *Ajuda online*.

Regras de validação da propriedade

É possível definir regras de validação para restringir os valores de propriedade que os usuários podem inserir para um conjunto predefinido de valores selecionáveis. Por exemplo, se você definiu uma propriedade chamada Sistema operacional, poderá definir a regra de validação como uma lista suspensa contendo as opções Windows, UNIX e Linux.

Propriedades definidas sem regras de validação são apresentadas ao usuário como caixas de texto livre, que permitem que qualquer sequência de caracteres seja informada. As regras de validação podem tornar a elaboração de relatórios sobre valores de área e categoria menos complexa e propensa a erros.

Observação: as regras de validação de propriedade são reutilizáveis. Elas não são específicas para uma propriedade em particular. É possível aplicar qualquer regra de validação existente a propriedades definidas para categorias de mudança, categorias de ocorrência ou áreas de solicitação/incidente/problema.

Dependendo do tipo de regra de validação que você configurou para uma propriedade, quando o usuário atribuir um ticket à categoria ou área a que essa propriedade está anexada, um dos seguintes controles é exibido na guia de propriedades do ticket:

- Text Edit Box—nenhuma regra de validação foi definida e nenhum valor padrão pode ser especificado. Espera-se que os usuários insiram valores que sigam os exemplos fornecidos por você.
- Check Box—uma caixa de seleção de dois estados é exibida na guia Propriedades. Por padrão, a caixa de seleção não está marcada. O usuário pode aceitar o padrão ou marcar a caixa de seleção. As caixas marcadas são exibidas na página de detalhes do ticket com Sim na coluna Valor. Caixas desmarcadas são exibidas com um Não na coluna de valor.
- Drop-down List—uma lista suspensa contendo um conjunto predefinido de opções é exibida na guia Propriedades. Se você tiver definido um valor padrão, ele será selecionado quando a lista suspensa for exibida pela primeira vez. A opção que o usuário seleciona é mostrada na coluna Valor da página de detalhes do ticket.

Defina as categorias de mudança e ocorrência para um autoatendimento

É possível usar a opção Inclusão de autoatendimento para definir quais categorias de mudança e ocorrência incluir nos tickets para autoatendimento. Também é possível definir diferentes símbolos de autoatendimento em comparação àqueles vistos pelo analista. Quando o ticket é salvo, o símbolo do autoatendimento é exibido no campo da Categoria mudança (ou Ocorrência). Se o ticket é exibido na interface do analista, o símbolo normal para a categoria aparece.

Para definir uma mudança (ou ocorrência) para autoatendimento

1. Na guia Administração, selecione Service Desk, Requisições de mudança (ou Ocorrências), Categorias.

   A página Lista de categorias é exibida.

2. Selecione Editar na lista.

   A parte superior da página exibe os campos editáveis.

3. Selecione a categoria desejada na lista Símbolo.

4. Preencha os seguintes campos:

   Inclusão de autoatendimento

   Especifica se essa categoria é mostrada na interface de autoatendimento.

   Padrão: Sim

   Símbolo de autoatendimento

   Especifica um identificador único para essa categoria na interface de autoatendimento..

   Ativo

   Especifica se a categoria está ativa ou inativa.

   A categoria é definida para autoatendimento.

5. Clique em Salvar.

   A categoria atualizada aparece na Lista de categorias de mudança (ou ocorrência) quando você reexibe a lista.

Fechamento automático de tickets

Você pode usar uma definição configurável para permitir o fechamento automático de tickets (solicitações/incidentes/problemas, requisições de mudança ou ocorrências). Quando um ticket é configurado para um status Resolvido, o ticket é automaticamente fechado no número de horas comerciais especificado. A notificação de atividade Fechamento automático enviada ao usuário final exibe o número de horas comerciais antes que o ticket seja fechado. O número de horas é configurável e específico do inquilino. Se o status for alterado antes de o número configurável de horas terminar, o fechamento do ticket é cancelado.

Administradores podem realizar as seguintes ações:

- Defina uma configuração de Fechamento automático para controlar o número de horas comerciais, para o usuário final, antes que o ticket seja automaticamente fechado.
- Configure uma notificação de atividade de Fechamento automático para notificar os contatos apropriados quando o fechamento automático estiver programado para um ticket.

Se você usa multilocação, considere o seguinte:

- O sistema usa a configuração pública padrão de Fechamento automático quando uma configuração de Fechamento automático específica do inquilino não é encontrada.
- Há uma configuração de Fechamento automático para cada inquilino.

Observação: para obter informações mais detalhadas sobre como executar esses procedimentos, consulte as informações de Configurações de fechamento automático na *Ajuda online*.

Mais informações:

Como definir configurações de ticket de fechamento automático (na página 328)
Como definir uma notificação de atividade de fechamento automático (na página 329)

Como definir configurações de ticket de fechamento automático

Você pode definir o número de horas comerciais antes de um ticket ser fechado (todos os tipos de ticket) como segue:

1. Na guia Administração, selecione Service Desk, Dados de aplicativo, Códigos, Fechamento automático.
2. Clique em Criar novo na página de lista.
3. Preencha os seguintes campos na página de detalhes:

   Símbolo

   Define o nome de configuração do sistema.

   Solicitação/Incidente/Problema/Requisição de mudança/Ocorrência

   Define o número de horas comerciais após um ticket ser definido para definir o status Resolvido antes de o ticket ser fechado. Se o status for alterado antes de o número de horas terminar, o fechamento do ticket é cancelado. 0 (zero) hora indica que fechamento automático não está implementado para o tipo de ticket.

   Descrição

   Fornece uma descrição breve do registro.

   Status

   Indica se o registro está ativo ou inativo.

   A configuração de fechamento automático é definida.
4. Clique em Salvar, Fechar janela.

   A nova configuração aparece na página Lista de fechamento automático quando você exibe novamente a lista.

Como definir uma notificação de atividade de fechamento automático

Você pode alterar as configurações na notificação de atividade de fechamento automático padrão para notificar os contatos adequados quando o fechamento automático está programado para um ticket. A atividade é válida para todos os tipos de ticket do CA SDM, e inclui uma regra de notificação padrão para solicitações/incidentes/problemas, requisições de mudança e ocorrências.

Para definir uma notificação de atividade de fechamento automático, faça o seguinte:

1. Na guia Administração, selecione Notificações, Notificações de atividade.
2. Selecione a notificação de atividade de Fechamento automático na página de lista para abri-la.
3. Atualizar a Regra de notificação de fechamento automático padrão e especificar contatos para receber a notificação.
4. Clique em Salvar, Fechar janela.

   A notificação de atividade de Fechamento automático atualizada aparecerá na Lista de notificações de atividade quando você exibir novamente a lista.

Atividades de ticket relacionadas

Quando uma atividade é gerada para um ticket do CA SDM, você pode propagar a atividade para um ou mais tickets relacionados. Por exemplo, um registro de problema criado a partir de um Incidente pode atualizar o registro de incidentes quando o problema for resolvido. Quando a atividade ocorre, é gerado um log de atividade para o ticket relacionado que inclui as seguintes informações:

- O tipo de atividade do ticket relacionado, por exemplo, Atualizar status
- Nome do contato
- Tipo de ticket pai e seu número de referência
- Descrição do log da atividade, por exemplo, status atualizado de Trabalho em andamento para Aberto

Os logs de atividade são propagados para tickets relacionados com base nas propriedades definidas dentro de cada notificação de atividade. Os atributos dos respectivos tickets não são modificados. Os seguintes relacionamentos são propagados:

- Problemas são propagados para todos os Incidentes ativos.
- Requisições de mudança são propagadas para todos os Problemas e Incidentes ativos.

Como administrador de sistema, você pode executar as seguintes ações:

- Definir as notificações de atividade para propagar atividades relacionadas ao ticket.
- Configurar uma notificação de atividade de um Ticket relacionado para notificar os contatos adequados quando a atividade for propagada para tickets relacionados.

Observação: para obter informações mais detalhadas sobre como executar esses procedimentos, consulte as informações de Notificações de atividade na *Ajuda online*.

Mais informações:

Registro de atividades (na página 464)
Como definir notificações de atividade para tickets relacionados (na página 331)
Como definir notificações de atividade de ticket relacionadas (na página 332)

Como definir notificações de atividade para tickets relacionados

Você pode propagar logs de atividade para tickets relacionados com base nas propriedades definidas em cada notificação de atividade. Os atributos dos respectivos tickets não são modificados.

Para definir uma notificação de atividade para atividades de ticket relacionadas, faça o seguinte:

1. Na guia Administração, selecione Notificações, Notificações de atividade.
2. Abra a notificação de atividade apropriada para edição.
3. Na página de detalhes, clique na caixa de seleção Atividade do ticket relacionado para marcá-la com ativa.

   Observação: Se usar multilocação, faça o seguinte:

   - Especifique o tipo de inquilino apropriado na lista suspensa Atividade do ticket relacionado.
   - Digite o nome do inquilino no campo inquilino ou clique no ícone pesquisa para pesquisar um inquilino.
4. (Opcional) Atualizar a Regra de notificação padrão e especificar contatos para receber a notificação.
5. Clique em Salvar, Fechar janela.

   A notificação de atividade atualizada aparecerá na Lista de notificações de atividade quando você exibir novamente a lista.

Como definir notificações de atividade de ticket relacionadas

Você pode alterar a configuração padrão na notificação de atividade de Ticket relacionado para notificar os contatos apropriados quando os logs de atividade forem propagados para tickets relacionados (solicitações/incidentes/problemas, requisições de mudança e ocorrências).

Para definir uma notificação de atividade de ticket relacionada, faça o seguinte:

1. Abra a notificação de atividade de Tickets relacionados na página Lista de Notificações de Atividade.
2. Clique em Editar e altere um ou mais dos campos conforme o caso na página de detalhe.
3. (Opcional) Atualizar a Regra de Notificação padrão para e especificar os contatos a receberem notificação.
4. Clique em Salvar, Fechar janela.

   A notificação de atividade de Ticket relacionado atualizada aparecerá na Lista de notificações de atividade quando você exibir novamente a lista.

Cálculo de prioridade

Cálculo de prioridade é um conjunto predefinido de valores que automaticamente configura os campos Prioridade, Urgência e Impacto em problemas e incidentes. O cálculo de prioridade ajuda no gerenciamento de incidentes e problemas para suas necessidades de negócios e recursos de TI. ITIL recomenda a priorização dos tickets usando um cálculo de dados com base em valores de Urgência e Impacto. As organizações de suporte definem esse cálculo com base em seus processos exclusivos, como esse cálculo determina os SLAs (Contratos de Nível de Serviço) e outros eventos importantes do sistema. Esse cálculo pode incluir o estado crítico do IC vinculado ao incidente e ao problema. Priorizando tickets de forma eficaz ajuda você a fazer o seguinte:

- Alocar recursos de TI para tickets
- Atender melhor os clientes
- Reduzir os custos

A solução do CA SDM para cálculo de prioridade inclui os seguintes componentes:

- Uma Matriz de cálculo de prioridade com base nos valores de Urgência e Impacto
- Valores padrão de Urgência e Impacto
- Opções de ajuste de Urgência e Impacto com base em Serviço afetados, data de abertura, Usuário final afetado, a área de incidente ou problema
- Uma opção para Capturar o motivo para modificar, manualmente, a Urgência ou o Impacto
- Uma opção Ativar para modelos para a criação de um ticket a partir de um modelo

Quando você instala o CA SDM, um cálculo de prioridade Padrão automaticamente gerencia os valores do ticket. É possível modificar as configurações de cálculo de prioridade Padrão, ou criar cálculos de prioridade adicionais para gerenciar incidentes ou problemas. No cálculo de prioridade, você define o resultado com base nos cenários de negócios para tornar o nível de importância e o processamento do ticket mais consistentes. Os usuários podem substituir algumas configurações, mas não podem mais definir a Prioridade no ticket porque esse valor é conduzido por dados. Para multilocação, você ou os inquilinos podem criar cálculos de prioridade adicionais com configurações específicas para cada inquilino.

Quando um analista abre um incidente ou problema, o sistema automaticamente um cálculo de prioridade ativo e valores de ticket para gerar configurações de Prioridade, Urgência e Impacto. As configurações são baseadas em um ou mais dos seguintes campos:

- Urgência
- Impacto
- Usuário final afetado
- Área de incidente ou problema
- Data de abertura
- Serviço afetado

Os analistas podem substituir os valores Urgência e Impacto conforme o necessário. Dependendo de como você configura o Gerenciador de opções, os funcionários apenas podem substituir os valores de Urgência de incidente quando a opção *urgency_on_employee* estiver instalada. Quando o sinalizador Capturar razão estiver ativado e os usuários substituírem os valores de Urgência ou de Impacto e clicarem em Salvar, a página Escalate Detail será exibida para permitir que os usuários descrevam um motivo para a mudança.

Todos os cálculos de prioridade do ticket, substituições manuais e informações de razão aparecem no Novo log de atividade. Se não ocorrer nenhum ajuste de cálculo de prioridade, o sistema não cria uma entrada de log de atividade.

Observação: se você migrou de uma versão anterior, o cálculo de prioridade está desativado por padrão. Para obter informações sobre como ativar o cálculo de prioridade ou reter suas personalizações, consulte o *Guia de Implementação*.

Como o cálculo de prioridade gerencia valores de ticket

O sistema ajusta valores de problema e incidente com base em configurações de cálculo de prioridade ativo para ajudar os Analistas a tratar tickets de forma mais efetiva. A tabela a seguir resume como o cálculo de prioridade modifica campos com base no cálculo de prioridade e ações de usuário para problemas, incidentes, serviço web, email e a API de texto:

Ação	Automático Mudanças no campo	Descrição
O usuário altera o Serviço afetado	Impacto Prioridade	O sistema avalia o valor de Impacto do serviço no IC do tipo Serviço para calcular o novo valor de Impacto. Os ICs do tipo de Serviço são definidos como ICs que têm sua classe definida na família de Serviço empresarial. Se a data de abertura do ticket estiver dentro do intervalo de tempo da janela de interrupção, o sistema incrementa um novo valor de Impacto com base no campo Incremento do impacto. O sistema só substitui o valor do Impacto quando o novo valor é maior que o valor de impacto inicial.
O usuário altera a Área de incidente	Urgência	O valor de Urgência é modificado somente quando o novo valor é maior do que o valor padrão.

Ação	Automático Mudanças no campo	Descrição
O usuário altera a Área de incidente *e* o Usuário final afetado	Urgência Prioridade	Se o usuário definir o campo Área de incidente primeiro, o valor Urgência é alterado depois que o usuário definir o Usuário final afetado. O cálculo de prioridade define a Prioridade.
O usuário altera Urgência *e* Impacto	Prioridade Impacto	O sistema avalia o valor de Impacto do serviço no IC do tipo Serviço para calcular o novo valor de Impacto. Se a data de abertura do ticket estiver dentro do intervalo de tempo definido por uma janela de interrupção, o sistema incrementa um novo valor de Impacto com base no campo Incremento do impacto. O sistema só substitui o valor do Impacto quando o novo valor é maior que o valor de impacto inicial. Se o Administrador definir o Motivo da captura, o usuário deverá fornecer um motivo para a modificação. Se o usuário modificar os valores Urgência e Impacto, estes valores permanecem os mesmos durante toda a criação ou atualização do ticket, a não ser que o usuário modifique-os novamente. No entanto, o sistema pode atualizar valores sobrescritos para Urgência ou Impacto na próxima vez que o usuário atualizar o ticket. Depois que o sistema ajusta Urgência e Impacto, o cálculo de prioridade define o valor de Prioridade.
O usuário seleciona Novo incidente com base no Documento de conhecimento e o sistema tem substituições para Documentos de conhecimento (na página 344)	Impacto Urgência	O sistema sempre usa os valores Documento de conhecimento ou solução de conhecimento, independentemente se os valores são maiores ou menores do que os valores padrão do cálculo de prioridade. Por exemplo, se um cálculo de prioridade tem um valor de Impacto de 3-Grupo único e valor de Urgência de 3-Rápido, e os Documentos de conhecimento têm um valor de Impacto de 2-Vários grupos e valor de Urgência de 4-Muito rápido, o sistema aplica os valores do Documento de conhecimento ao incidente. O valor da prioridade é sempre produzido a partir cálculo de prioridade.

Ação	Automático Mudanças no campo	Descrição
O usuário aceita o Documento de conhecimento como solução para o problema ou incidente	Impacto Urgência	O sistema usa os valores do Documento de conhecimento para Impacto e Urgência. O sistema também usa o cálculo de prioridade para definir o valor da Prioridade.
O usuário deriva o incidente do Documento de conhecimento selecionando Novo Incidente	Impacto Urgência Prioridade	O sistema usa os valores de cálculo de prioridade.
O usuário produz o incidente a partir do Documento de conhecimento sem as substituições de Documentos de conhecimento (na página 344) pelo sistema.	Impacto Urgência Prioridade	O sistema usa os valores de cálculo de prioridade independentemente de como o usuário criou o incidente para o Documento de conhecimento ou solução de conhecimento.
O ticket aceita o Documento de conhecimento como solução para o problema ou incidente e o sistema não substitui para documentos de conhecimento	Impacto Urgência Prioridade	O sistema usa valores de problema ou incidente. O valor de Prioridade origina-se do cálculo de prioridade.
O ticket que está em Modo somente leitura aceita o Documento de conhecimento como solução para o problema ou incidente e o sistema substitui para Documentos de conhecimento	Impacto Urgência Prioridade	O sistema usa os valores de Impacto e Urgência do Documento de conhecimento se eles não estiverem vazios. Se o valor de Impacto/Urgência no Documento de conhecimento estiver vazio, o sistema usa os valores do problema ou do incidente. O valor de Prioridade origina-se do cálculo de prioridade.
O ticket que está em Modo edição aceita o Documento de conhecimento como solução para o problema ou incidente e o sistema substitui para Documentos de conhecimento	Impacto Urgência Prioridade	O sistema usa valores de problema ou incidente. O valor de Prioridade origina-se do cálculo de prioridade.

O cálculo de prioridade gera valor de urgência depois de salvar tickets de autoatendimento

Por projeto, o cálculo de prioridade gera valores de urgência somente após os usuários do autoatendimento salvarem os incidentes. Usuários do autoatendimento, como funcionários VIP, funcionários e usuários anônimos, podem exibir o valor gerado depois de salvar um ticket.

Para usuários do autoatendimento, o cálculo de prioridade usa as seguintes configurações e valores para gerar valores de urgência:

- Urgency_On_Employee é definido como Sim no Gerenciador de opções
- O valor Urgência da substituição está ativado no cálculo de prioridade ativo para incidentes
- *Web.cfg* Configurações de urgência como AnonymousUrg para usuários anônimos, ESCEmpUrg para funcionários VIP e EmpUrg para todos os outros funcionários
- Valores de urgência da área
- Substituições manuais do usuário

A seguinte tabela resume como o cálculo de prioridade define o valor de urgência para incidentes de autoatendimento:

Ação do usuário de autoatendimento	Valor de urgência
O usuário salva um incidente com a urgência padrão e uma Área de incidente vazia.	O ticket mostra o valor de urgência padrão do *web.cfg*.
O usuário salva um incidente depois de substituir o valor de urgência.	Independentemente da Urgência da área, *web.cfg*, ou das configurações de cálculo de prioridade, o ticket mostra o valor de urgência que o usuário selecionou.
O usuário salva um incidente depois de selecionar uma Área de incidente. A Área de incidente não possui um valor de Urgência da área predefinido.	O ticket mostra o valor de urgência padrão do *web.cfg*.
O usuário salva um incidente depois de selecionar uma Área de incidente que possui um valor de Urgência da área predefinido. A opção Urgência da substituição também está ativada no cálculo de prioridade ativo de incidentes.	Se o valor de Urgência da área for maior que a urgência em *web.cfg*, o ticket mostra o valor de Urgência da área. Entretanto, o campo Urgência atualizado não está visível enquanto o usuário está criando ou editando o ticket. Quando o usuário salva e abre novamente o incidente, o valor de Urgência atualizado aparece no incidente.

Ação do usuário de autoatendimento	Valor de urgência
O usuário salva um incidente depois de selecionar uma Área de incidente que possui um valor de Urgência da área predefinido. Entretanto, a opção Urgência da Substituição está desativada no cálculo de prioridade ativo de incidentes.	O ticket mostra um valor de Urgência do *web.cfg*.
O usuário edita um incidente existente que possui uma área de incidente com um valor de Urgência da área predefinido.	A lista suspensa Urgência mostra o valor Urgência da área e todos os valores do *web.cfg* aplicáveis.

Observação: para obter informações sobre a configuração dos valores de Urgência para usuários de autoatendimento, consulte o *Guia de Implementação*.

Como definir o cálculo de prioridade

Por padrão, os valores de ticket, como prioridade, são baseados em um cálculo de prioridade. Você pode encontrar e ajustar os valores iniciais para Prioridade e Urgência em web.cfg. O web.cfg possui configurações separadas para diversos usuários, como convidado, usuário VIP e funcionário.

Observação: se você migrou de uma versão anterior, o cálculo de prioridade está desativado por padrão. As páginas Customized Incident e Detalhes do problema problemas exigem configuração adicional para funcionar adequadamente. Para obter informações sobre como ativar o cálculo de prioridade ou reter suas personalizações, consulte o *Guia de Implementação*.

Para definir o cálculo de propriedades, faça o seguinte:

1. Na guia Administração, selecione Service Desk, Solicitação/Incidente/Problema, Cálculo de prioridade.

   A Lista de Cálculo de Prioridade aparece.

2. Clique com o botão direito do mouse em cálculo de prioridade padrão e selecione Editar a partir do menu de atalho.

   A página Detalhes do cálculo de prioridade padrão mostra configurações padrão para tickets de incidente e problema.

3. Revise o cálculo de prioridade padrão e ajuste os valores de acordo. Ao configurar os valore do cálculo de prioridade padrão, considere as seguintes ocorrências para seu ambiente de trabalho.
   - **Escalonamento de ocorrência**—Quando tickets exibem escalonamento para um VIP em particular, é possível aumentar o valor para Urgência.
   - **ICs cruciais**—Para ICs cruciais, é possível configurar o Impacto de serviço para cada IC.
   - **Tempo de funcionamento de serviço crucial**—Quando os ICs exibem alta disponibilidade, adicione uma janela de blackout.
   - **Janela de blackout**—Quando tickets relacionados a CI são usados para uma janela de blackout em particular, é possível aumentar o valor de Impacto de serviço no cálculo de prioridade.
4. Use a configuração Substituir manualmente para permitir aos usuários alterar a configuração de tickets conforme o necessário.
5. Se desejar um cálculo de prioridade separado para gerenciar problemas ou incidentes, configure o tipo de ticket (na página 342).
6. Clique em Salvar.

   No ticket ou Documento de conhecimento seguinte ou atualizado, os campos se atualizam conforme os valores no cálculo de prioridade ativa.
7. Considere criar cálculos de prioridade adicionais para cada tipo de ticket. Para multilocação, crie e ative cálculos de prioridade adicionais para gerenciar tickets para cada inquilino.

Observação: para obter informações sobre cálculo de prioridade, consulte a *Ajuda online*.

Cálculos de várias prioridades

É possível definir mais de um cálculo de prioridade. No entanto, somente um cálculo de prioridade ativo controla problemas ou incidentes ou ambos. Por exemplo, é possível ter um cálculo de prioridade ativo para problemas e outro para incidentes. Também é possível ter vários cálculos de prioridade inativos para uso futuro.

Atribuição de cálculo de prioridade para multilocação

Você ou seus inquilinos podem criar cálculos de prioridade específicos de inquilino para gerenciar incidentes e problemas. Quando você atribuir cálculos de prioridade para multilocação, considere o seguinte:

- Quando um cálculo de prioridade não tiver um inquilino atribuído, ele será considerado público. O status de um cálculo de prioridade público é Ativo ou Inativo. Um cálculo de prioridade não será mais considerado público quando ele for atribuído a um inquilino.
- Se um inquilino não tiver atribuição de cálculo de prioridade, o cálculo de prioridade Padrão ou outro cálculo de prioridade público ativo irá automaticamente gerenciar problemas e incidentes.
- Um cálculo de prioridade gerencia problemas e incidentes para um inquilino. No entanto, um cálculo de prioridade específico de inquilino separado pode controlar cada tipo de ticket. Por exemplo, a Empresa X tem um cálculo de prioridade para controlar incidentes e outro para gerenciar problemas.
- Quando inquilinos criam seus próprios cálculos de prioridade enquanto cálculos de prioridade públicos estão ativos, o cálculo de prioridade específico de inquilino aplica-se somente aos tickets do inquilino correspondente.

  Por exemplo, se o cálculo de prioridade Padrão estiver ativo, o inquilino da Empresa X pode criar um cálculo de prioridade específico de inquilino chamado new_priority_calculation. As novas definições e configurações do new_priority_calculation aplicam-se somente aos incidentes e problemas da Empresa X.
- Se o inquilino desativar um cálculo de prioridade, o sistema usará um cálculo de prioridade público ativo para gerenciar problemas e incidentes.

  Por exemplo, a Empresa X desativa o cálculo de prioridade específico de inquilino enquanto ainda há um cálculo de prioridade Padrão ativo. O cálculo de prioridade permanece ativado para a Empresa X, pois o sistema usa o cálculo de prioridade Padrão para gerenciar incidentes e problemas para a Empresa X.

  Observação: como inquilinos podem excluir seus próprios registros de cálculo de prioridade, recomendamos que você desative os cálculos de prioridade públicos que gerenciam incidentes e problemas. Em vez disso, você ou os inquilinos podem criar cálculos de prioridade específicos de inquilino.

- Quando você desativa a multilocação e há mais do que um cálculo de prioridade ativo que gerencia inquilinos, deixe *apenas um* cálculo de prioridade para gerenciar incidentes e problemas. Por exemplo, é possível desativar todos os cálculos de prioridade, exceto um, para gerenciar incidentes, e outro para lidar com problemas.

Observação: para obter informações sobre multilocação, consulte o *Guia de Implementação*.

Como atribuir um Inquilino a um Cálculo de prioridade

Para multilocação, é possível atribuir um inquilino a um cálculo de prioridade. Em primeiro lugar, você desativa os cálculos de prioridade pública. A seguir, você atribui o inquilino a um cálculo de prioridade e o ativa.

Para atribuir um inquilino a um cálculo de prioridade, faça o seguinte:

1. Na guia Administração, selecione Service Desk, Solicitação/Incidente/Problema, Cálculo de prioridade.

   A Lista de Cálculo de Prioridade aparece.

2. Edite cada cálculo de prioridade pública como, por exemplo, Padrão. Defina o status como Inativo e clique em Salvar.

   O sistema desativa os cálculos de prioridade pública.

3. Para cada inquilino, crie ou edite um cálculo de prioridade com configurações específicas do inquilino para Impacto, Urgência e Prioridade.

   A página Create Priority Calculation ou Atualizar cálculo de prioridade é exibida.

4. No campo Nome, especifique o inquilino:
5. No campo Status, selecione Ativo.
6. Clique em Salvar.

   O sistema aplica valores específicos de inquilino para Impacto, Urgência e Prioridade em novos incidentes e problemas.

Observação: para obter informações sobre criação e edição de cálculos de prioridade, consulte a *Ajuda online*.

Considerações de tipo de ticket para cálculo de prioridade

Ao configurar os tipos de ticket para um cálculo de prioridade, considere o seguinte:

- O cálculo de prioridade padrão permite gerenciar tipos de ticket tanto de incidente quanto de problema.
- Se você está migrando de um release anterior, ativa o cálculo de prioridade padrão ou cria um cálculo de prioridade para gerenciar problemas e incidentes.
- Embora você possa ter muitos cálculos de prioridade, somente um cálculo de prioridade ativo pode processar um tipo de ticket em particular. Por exemplo, um cálculo de prioridade ativo pode gerenciar problemas e outro pode gerenciar incidentes.
- Se você deseja criar um cálculo de prioridade e um cálculo de prioridade ativo já processa um tipo de ticket em particular, primeiro desative o tipo de ticket no cálculo de prioridade ativo. Por exemplo, se você deseja um cálculo de prioridade para gerenciar problemas, desativa o tipo de ticket de problema no cálculo de prioridade ativo e cria um cálculo de prioridade ativo que gerencie problemas.

Observação: para obter informações sobre a ativação de cálculo de prioridade e configuração de tipos de ticket durante a migração, consulte o *Guia de Implementação*.

Configurar tipos de ticket para um cálculo de prioridade

Você pode especificar os tipos de ticket que o cálculo de prioridade gerencia. Quando o cálculo de prioridade está ativo, ele gerencia os valores de Prioridade, Impacto e Urgência em novos tickets.

Para configurar tipos de ticket para um cálculo de prioridade

1. Na guia Administração, selecione Service Desk, Solicitação/Incidente/Problema, Cálculo de prioridade.

   A Lista de Cálculo de Prioridade aparece.

2. Clique com o botão direito do mouse em um cálculo de prioridade e selecione Editar.

   A página Atualizar cálculo de prioridade aparece.

3. Selecione ou desmarque uma ou mais das seguintes opções:

   Incidentes

   Ativa ou desativa esse cálculo de prioridade para gerenciar novos incidentes.

   Problemas

   Ativa ou desativa esse cálculo de prioridade para gerenciar novos tickets de problema.

4. Clique em Salvar.

   O CA SDM usa as configurações no cálculo de prioridade para gerenciar valores de ticket para novos incidentes, problemas ou ambos.

Usar modelos de ticket para calcular valores de prioridade

Se você deseja que modelos de ticket calculem prioridade, configure o cálculo de prioridade com a opção *Ativar para modelos*. Se essa opção for ativada, os valores Urgência e Impacto vêm do modelo, mas o campo prioridade vem do registro de cálculo de prioridade. O valor de prioridade é exibido como somente leitura.

Se você não ativar essa função, os campos Urgência, Impacto e Prioridade vêm do modelo. Você pode editar o campo de prioridade e nenhum cálculo de prioridade é realizado para o ticket até que ele seja salvo.

Para usar modelos de ticket para calcular valores de prioridade

1. Na guia Administração, selecione Service Desk, Solicitações/incidentes/problemas, Cálculo de prioridade.

   A Lista de Cálculo de Prioridade aparece.

2. Selecione o cálculo de prioridade que deseja usar para calcular a prioridade com modelos.

   Você também pode criar um cálculo de prioridade para usar modelos de ticket para calcular valores de prioridade.

3. Selecione *Ativar para modelos* a partir da lista Opções de cálculo de prioridade.

4. Clique em Salvar.

   A opção está ativada.

Usar Documentos de conhecimento para calcular valores de prioridade

Se você deseja que documentos de conhecimento calculem prioridade, é possível atualizar o mapeamento de campo. Após configurar o mapeamento de campo, o analista pode criar tickets de incidente ou problema a partir dos documentos de conhecimento. O documento de conhecimento calcula valores de Impacto e Urgência nos tickets. Se o valor de Impacto ou Urgência estiver faltando, os valores originam-se do cálculo de prioridade.

Importante: Se você modificar e salvar um ticket que já contém valores de Impacto e Urgência calculados por um documento de conhecimento, o cálculo de prioridade substitui os valores definidos pelo Gerenciamento de conhecimento. O log de auditoria exibe essas atividades.

Para usar documentos de conhecimento para calcular valores de prioridade

1. Na guia Administração, selecione Conhecimento, Integração com o Service Desk.
2. Selecione mapeamento de campo.

   A página Mapeamento de campo aparece.
3. Para Impacto e Urgência, marque as seguintes caixas de seleção conforme o adequado:

   Preencher os valores vazios do Service Desk

   Especifica se as informações do Gerenciamento de conhecimento devem ser usadas para preencher campos em ocorrências ou solicitações.

   Sobrescrever valores do Service Desk

   Identifica os campos em ocorrências ou solicitações que correspondem a campos listados na coluna do Gerenciamento de conhecimento.

   Observação: Quando o campo Override Service Desk values não estiver ativado, porém o campo Preencher valores vazios do Service Desk estiver ativado para Impacto e Urgência, os valores de conhecimento para Impacto e Urgência substituirão os valores de Incidente.
4. Clique em Salvar.

   Incidentes e problemas são criados usando os valores de Impacto e Urgência do documento de conhecimento para calcular o valor de Prioridade. Se os valores estiverem faltando, o ticket obtém os valores do cálculo de prioridade ativo. Se nenhum cálculo de prioridade estiver ativo para o tipo de ticket, o sistema limpa os campos de Prioridade, Urgência e Impacto.

Substituir manualmente o valor do impacto

Ao substituir manualmente o valor de Impacto em um problema ou incidente, o cálculo de prioridade ativo que gerencia o tipo de ticket automaticamente ajusta o valor da Prioridade.

Para substituir manualmente o valor de Impacto.

1. Abra a página de detalhes para o problema ou incidente que deseja alterar.
2. Alterar o valor de Impacto.

   Se houver um cálculo de prioridade ativo que gerencie o tipo de ticket, o valor de prioridade automaticamente se altera com base nas configurações do cálculo de prioridade.
3. Salvar o incidente.

   O Log de atividade na página Detalhes do incidente reflete as mudanças dos valores de Impacto.

Exemplo: substituir manualmente o valor de Impacto em um novo incidente.

1. Criar um incidente

   Por padrão, o valor de Urgência é 3-Rapidamente. O valor de Impacto é 3-Grupo único. O valor de Prioridade é 3.
2. Substitui o valor de Impacto para 1-Toda a organização.

   O valor de Prioridade automaticamente se altera com base nos valores no cálculo de prioridade ativa que gerencia incidentes.
3. Salvar o incidente.

   O Log de atividade na página Detalhes do incidente reflete as mudanças do Valor de impacto.

Substituir manualmente o valor de Urgência

Ao substituir manualmente o valor de Urgência em um ticket, o cálculo de prioridade ativo que gerencia o tipo de ticket automaticamente ajusta o valor da Prioridade.

Para substituir manualmente o valor de Urgência.

1. Abra a página de detalhes para o incidente que deseja alterar.
2. Alterar o valor de Urgência.

   Se houver um cálculo de prioridade ativo que gerencie o tipo de ticket, o valor de prioridade automaticamente se altera com base nas configurações do cálculo de prioridade.
3. Salvar o incidente.

   O Log de atividade na página Detalhes do incidente reflete as mudanças dos valores de Urgência.

Exemplo: substituir manualmente o valor de Urgência em um novo incidente.

1. Criar um incidente

   Por padrão, o valor de Urgência é 3-Rapidamente. O valor de Impacto é 3-Grupo único. O valor de Prioridade é 3.
2. Substitua o valor Urgência para 5-Imediato.

   O valor de Prioridade automaticamente se altera com base nos valores no cálculo de prioridade ativa que gerencia incidentes.
3. Salvar o incidente.

   O Log de atividade na página Detalhes do incidente reflete as mudanças no valor de Urgência.

Ajustar automaticamente o impacto para um problema ou incidente

Para Itens de configuração definidos com uma família de Serviços corporativos, é possível ajustar automaticamente o valor de Impacto para problemas ou incidentes. Ao selecionar a Área de problema ou incidente e selecionar um Serviço afetado, o impacto ajusta-se de acordo com as configurações de Impacto do serviço do IC para ICs de Serviço corporativo e para o cálculo de prioridade.

Para ajustar automaticamente o Impacto para um Problema de incidente

1. Criar um problema ou incidente para um IC de tipo de Serviço corporativo.
2. Selecione um serviço Afetado
3. Selecione uma Área de problema ou incidente.

   Se há um cálculo de prioridade ativo que gerencia o tipo de ticket, o valor do Impacto muda com base no valor do Aumento do impacto (usado para avaliação de impacto de Janela de blackout) no cálculo de prioridade e o valor do Impacto do serviço do serviço afetado.

   Se você está usando o cálculo de prioridade padrão, com um Impacto de serviço para o IC de serviço corporativo definido como 1-Toda a organização, e o Problema ou Incidente não está aberto em uma Janela de blackout, o valor de Impacto no Problema ou Incidente é definido como 1 e o valor de Prioridade no ticket é elevado para 2.
4. Salve o ticket.

   O Log de atividade na página Detalhes do incidente reflete as mudanças do valor de Impacto.

Ajustar o impacto para um Problema ou Incidente

O seguinte exemplo mostra como ajustar o impacto para um Problema ou Incidente.

1. Crie um Serviço corporativo CI chamado CI-APC e defina a casse como uma que venha abaixo do Serviço corporativo da família.

   Por exemplo, é possível definir a classe como Outros serviços, Serviços de negócio ou Serviços de infraestrutura.

2. Na guia Serviço, no formulário de Detalhes do IC, defina o campo Impacto de serviço para 2-Múltiplos grupos.

3. Na guia Service Desk, crie um incidente e define o Serviço afetado para CI-APC.

4. Salve o ticket.

   O campo Impacto no incidente reflete o valor para o Impacto de serviço do serviço afetado selecionado (CI-APC). Nesse caso, o valor Impacto é definido como 2 -Múltiplos grupos.

   Observação: se você está usando o cálculo de prioridade padrão e o ticket é criado durante um período de janela de blackout, o valor de Impacto aumenta em 1 e no caso acima, o valor de Impacto e definido como 1-Toda a organização.

Observação: para obter informações sobre a criação de ICs, consulte a Ajuda online.

Ajustar automaticamente a Urgência para um Problema ou Incidente

Para problemas e incidentes, você pode ajustar automaticamente Urgência e Prioridade especificado um usuário final afetado que requer Tratamento especial ou especificando uma Área de problema/incidente que possui um valor de Urgência de área.

Ao atribuir tratamento especial, com Escalonar urgência ativado, para um contato ou definir um valor de Urgência de área para uma área de problema/incidente, o valor Urgência em Problema/incidente ajusta-se automaticamente de acordo com os valores no cálculo de prioridade e o valor de Urgência de área para o usuário final afetado.

Para ajustar automaticamente a Urgência para um Problema ou Incidente

1. Criar um problema ou incidente.
2. Selecione um Usuário final afetado Para uma urgência elevada, selecione um Usuário final afetado que precise de Tratamento especial que tenha Escalonar urgência ativado.

   Se houver um cálculo de prioridade ativo que gerencie o tipo de ticket, o valor de Urgência mudará com base no valor de Incremento de urgência no cálculo de prioridade ativo.
3. Selecione uma Área de problema ou incidente.

   Se houver um cálculo de prioridade que gerencie o tipo de ticket, o valor Urgência muda com base no valor Urgência de área na definição de Área de problema/incidente.
4. Salve o ticket.

   Uma mensagem de confirmação lembra você de que o ticket requer tratamento especial. O Log de atividade na página Detalhes de problema/incidente reflete as mudanças no valor de Urgência.

Exemplo de ajustar a urgência para um problema ou incidente

O seguinte exemplo mostra como ajustar a urgência para um Problema ou Incidente.

1. Na guia Administrador, crie um contato chamado Não VIP.
2. Crie um contato de tratamento especial chamado VIP e defina o valor Escalonar urgência como ativado.
3. Crie uma área chamada Área de teste e especifique a Urgência da área como 2-Muito rápido.
4. Na guia Service Desk, crie um incidente.
5. Para o usuário final afetado, selecione Não VIP.
6. Na Área de incidente, selecione Área de teste e salve o ticket.

   O campo Urgência reflete o valor da Área de urgência a partir da definição de Área de incidente. Nesse caso, a Urgência é definida como 2-Muito rápido.

7. Alterar o usuário final afetado para VIP e salve o ticket.

   Se a matriz de Cálculo de prioridade está sendo usada, o valor de Urgência é incrementado em 1 e definido como 1-Imediato. Aparece uma mensagem de confirmação lembrando-o de que o ticket requer tratamento especial. O Log de atividade na página Detalhes do incidente reflete as mudanças do valor de Urgência

Observação: para obter informações sobre a criação de ICs, consulte a *Ajuda online*.

Transições de status e controles de atributos dependentes

Você também pode usar os seguintes controles configuráveis para restringir os fluxos de status de ticket para requisições de mudança, ocorrências, incidentes/problemas/solicitações e determinar quais campos são mostrados, ou obrigatórios para cada status de ticket:

Transições

Controla como os usuários selecionam os status disponíveis no formulário de incidente/problema/solicitação, ocorrência ou requisição de mudança. Por exemplo, um problema está em um status Aberto, e o fluxo de transição permite apenas que o analista atualize o status para Fechado. Neste exemplo, o analista não possui nenhuma outra opção de status, o que reforça o processo de gerenciamento de problemas.

As transições permitem definir um subconjunto da lista completa de status e especificar o novo (ou próximo) status padrão de um ticket com base no status atual. É possível definir transições de status exclusivas para cada tipo de ticket. Considere usar transições quando desejar restringir os fluxos de trabalho de status para seus usuários finais.

Atributos dependentes

Controla como os atributos são designados como obrigatórios (deve fornecer) ou bloqueados (não pode atualizar) dependendo do status do ticket. Por exemplo, o Gerenciador de mudanças pode impedir que um analista edite o atributo Resumo após uma requisição de mudança ser aprovada. Considere usar controles de atributo quando desejar restringir certos atributos com base no status.

Observação: é possível especificar com que rigidez o sistema impõe as diretivas de Status, configurando a opção Status Policy Violations no Gerenciador de opções (Opções gerais). Essa opção se aplica apenas a processos de sistema automatizados, tais como integrações e macros.

Mais informações:

Trabalhar com transições de status e Controles de atributos dependentes (na página 352)
Configurar transições de status (na página 352)
Melhor prática: Transições de status predefinidas (na página 360)

Trabalhar com transições de status e Controles de atributos dependentes

Para trabalhar com transições de status e controles de atributo dependentes, faça o seguinte:

1. Na guia Administração, configure os inquilinos, contatos e funções adequados para seu ambiente.
2. No nó Service Desk, especifique o tipo de ticket (Requisição de mudança, por exemplo) e selecione Status.

   A página Lista de status exibe códigos de status ativos.
3. Edite o código de status adequado (Confirmado, por exemplo) e use os controles disponíveis nas guias na parte inferior da página de detalhe de status do ticket para fazer o seguinte:
   - Configurar transições de status (na página 352)
   - Configurar controles de atributos dependentes (na página 354)

Observação: você pode configurar transições únicas e controles de atributo dependentes para cada tipo de ticket.

Configurar transições de status

É possível configurar um subconjunto da lista de status completa e especificar o próximo status padrão de um ticket com base no status atual. As transições são aplicadas quando o status é alterado no formulário de detalhes do ticket.

Para configurar transições de status

1. Clique na guia Transições na parte inferior da página de detalhes de status do ticket.

   A página Lista de transições mostra todas as transições válidas para o status.

   Observação: quando configurados, tipos de transição vinculados aparecem na lista Transição de incidente e solicitação.
2. Clique no botão Atualizar transação.

   A página Atualizar transições de status de ticket é exibida.

3. Configure as seguintes caixas de seleção conforme o adequado:

   Permitido

   Especifica uma transição válida para o status. Use esta opção para restringir os fluxos de trabalho de status.

   Padrão

   (Opcional) Especifica a transição de status padrão. O CA SDM aplica a transição padrão quando o usuário clica no botão de transição padrão no formulário de detalhes do ticket ou quando um usuário (incluindo um usuário de serviços web) atualiza o status para um valor <d>. Há apenas uma transição padrão para cada status (uma para cada inquilino em um sistema multilocação).

   Comentário obrigatório

   (Opcional) Especifica que um comentário de log de atividade para a transição é necessário ao alterar o status em um ticket.

   Observação: essa opção aplica-se somente a tickets do CA SDM. Não se aplica a outras áreas, como serviços web ou a funcionalidade de editar na lista.

4. (Opcional) Selecione um código de status na coluna Nome para atualizar seus detalhes.
5. Clique em Salvar.

   A lista de transições configurada para o novo status é exibida na lista de Transição. Quando o analista seleciona a lista suspensa Status no formulário de ticket, a nova lista de status é exibida.

Observação: para obter informações detalhadas de procedimento sobre definir transições de status, consulte a *Ajuda online*.

Configurar controles de atributos dependentes

Você pode determinar que campos são mostrados ou obrigatórios para o status d ticket.

Observação: antes de configurar atributos dependentes como "obrigatórios" para o status do ticket, esteja ciente de que a opção Editar na lista que aparece na página de lista do ticket pode não exibir os valores de campo de atributo obrigatórios. Se o valor de campo de atributo obrigatório ainda não for parte do ticket salvo, e se não for apresentado no formato Editar na lista, o ticket não será salvo. Consequentemente, o analista deve editar os valores do campo atributo dependente na página de detalhes do ticket em vez de usar a opção Editar na lista.

Para configurar um controle de atributo dependente

1. Na página de detalhes de status do ticket, selecione a guia Controle de atributo dependente na parte inferior da página.

   A Lista de controles de atributo aparece.

2. Clique em Criar.

   A página Update status dependent attribute control é exibida.

3. Preencha os seguintes campos:

   Inquilino

   (Opcional) Em um sistema com multilocação instalado, especifica um nome de inquilino opcional. Se um inquilino for especificado, a dependência aplica-se somente àquele inquilino e aos seus subinquilinos.

   Atributo

   Especifica o nome do atributo que você deseja controlar, por exemplo, Resumo.

   Bloqueado

   Especifica o atributo como bloqueado. Um atributo bloqueado associado com um status não pode ser atualizado em um ticket com o mesmo status. O atributo está desbloqueado quando o status é alterado.

   Obrigatório

   Especifica o atributo como obrigatório. Um atributo obrigatório para o status não pode usar um valor nulo em um ticket com o mesmo status.

4. Clique em Salvar.

   O novo controle de atributo para o status é exibido na Lista de controle de atributo quando você exibe a página novamente. Quando um usuário atualiza o status do ticket, o sistema recupera a lista de atributos obrigatórios correspondentes ao novo status e atualiza o formulário de ticket conforme o adequado. Uma mensagem de erro aparece na parte superior do formulário de ticket quando um usuário tenta fechar o ticket sem preencher um campo obrigatório.

Observação: para obter informações detalhadas de procedimento sobre definir controles de atributo dependentes, consulte a *Ajuda online*.

Métodos de serviços web

É possível configurar os seguintes métodos de serviços web de transição de status e controle de atributo dependente:

getValidTransitions

Lista as transições de um ticket. Esse método é modelado no método getValidTaskTransitions existente, exceto que o argumento pode ser um ticket ou um status.

getDependentAttrControls

Lista os atributos bloqueados e obrigatórios para o atributo de um objeto com ID persistente especificado. O atributo Status é suportado neste momento.

Observação: para obter mais informações sobre métodos de serviços web SOAP, consulte o *Guia de Referência técnica*.

Fluxos de transição predefinidos

Para cada tipo de ticket, é possível usar as transições de status predefinidas fornecidas com o produto e modificá-las para acomodar seu fluxo de transição desejado.

Observação: uma vez que transições de status podem ser compartilhadas entre integrações, como CA Workflow, não torne inativas transições de status predefinidas, a menos que explicitamente solicitado.

Para visualizar a lista de transições predefinidas, faça o seguinte:

Na guia Administração, expanda o nó Service Desk e selecione entre:

- Transições de requisição de mudança
- Transições da ocorrência
- Transições de Solicitação/Incidente/Problemas

A Lista de transições exibe as transições predefinidas que permitem controlar como um ticket (incidente/solicitação/problema, requisição de mudança e ocorrência) segue através do seu ciclo de vida.

Observação: para obter informações detalhadas de procedimento criar e modificar transições, consulte a *Ajuda online*.

Fluxo de transição Incidente

A tabela a seguir mostra o fluxo de transição Incidente predefinido.

Status atual	Transição padrão	Próximos status disponíveis
Confirmada	Em andamento <d>	Evitada, Aguardando Fornecedor, Cancelada, Fechada, Fechada não resolvida, Em andamento, Aberta, Mudança pendente, Resolvida
Evitado		Confirmada, Evitada, Aguardando resposta do usuário final, Fechada, Fechada não resolvida, Em andamento, Solução rejeitada, Pesquisando, Resolvida
Aguardando resposta do usuário final	Pesquisando <d>	Fechada, Fechada não resolvida, Em andamento, Aberta, Pesquisando, Resolvida
Aguardando fornecedor	Pesquisando <d>	Confirmada, Fechada, Fechada não resolvida, Em andamento, Aberta, Mudança pendente, Pesquisando, Resolvida

Status atual	**Transição padrão**	**Próximos status disponíveis**
Cancelado		Fechado
Fechado		Abrir
Fechado, sem resolução		Confirmada
Fechado, sem resolução		Fechado
Fechado, sem resolução		Abrir
Em espera		Confirmado, fechado, em andamento, aberto, mudança pendente, resolvido
Em andamento	Pesquisando <d>	Confirmado, aguardando resposta do usuário final, aguardando fornecedor, fechado, fechado sem resolução, aberto, mudança pendente, pesquisando, resolvido
Mudança pendente	Pesquisando <d>	Confirmada, Fechada, Em andamento, Aberta, Resolvida
Pesquisando	Resolvido <d>	Fechada, Aberta, Resolvida
Resolvido	Fechado <d>	Aguardando resposta do usuário final, Fechada, Aberta

Fluxo de transição de problema

A tabela a seguir mostra o fluxo de transição Problema predefinido.

Status atual	**Transição padrão**	**Próximos status disponíveis**
Confirmada	Em andamento <d>	Confirmada, Aprovada, Cancelada, Fechada, Correção em andamento, Aberta, Rejeitada, Pesquisando
Análise concluída	Aprovado <d>	Confirmada, Cancelada, Fechada, Correção em andamento
Aprovado	Correção em andamento <d>	Fechada, Corrigida, Mudança pendente
Aguardando fornecedor	Pesquisando <d>	Confirmada, Fechada, Fechada não resolvida, Corrigida, Em andamento, Aberta, Mudança pendente, Pesquisando
Cancelado	Fechado <d>	Fechado, fechado, sem resolução, aberto

Status atual	Transição padrão	Próximos status disponíveis
Fechado, sem resolução		Confirmado, fechado, aberto
Correção em andamento	Corrigido <d>	Aprovada, Cancelada, Corrigida, Correção em andamento, Pesquisando, Rejeitada
Fixo	Fechado <d>	Fechado
Em espera	Pesquisando <d>	Confirmada, Fechada, Corrigida, Em andamento, Aberta, Mudança pendente, Pesquisando
Em andamento	Pesquisando <d>	Confirmada, Aprovada, Cancelada, Fechada, Correção em andamento, Mudança pendente, Rejeitada, Pesquisando
Erro conhecido	Correção em andamento <d>	Fechada, Correção em andamento, Corrigida
Abrir	Confirmado <d>	Confirmada, Aprovada, Cancelada, Fechada, Correção em andamento, Em andamento, Rejeitada, Pesquisando
Mudança pendente	Corrigido <d>	Fechada, Corrigida, Pesquisando
Rejeitado	Fechado <d>	Fechado, fechado, sem resolução, aberto
Pesquisando	Análise concluída <d>	Confirmada, Análise concluída, Aprovada, Cancelada, Fechada, Correção em andamento, Corrigida, Rejeitada

Fluxo de transição da ocorrência

A tabela a seguir mostra o fluxo de transição da ocorrência predefinido.

Status atual	Transição padrão	Próximos status disponíveis
Confirmada	Em andamento <d>	Aguardando resposta do usuário final, Aguardando fornecedor, Fechada, Fechada não resolvida, Em andamento, Aberta, Mudança pendente, Resolvida
Aguardando resposta do usuário final	Pesquisando <d>	Confirmada, Fechada, Fechada não resolvida, Em andamento, Aberta, Pesquisando, Resolvida
Aguardando fornecedor	Pesquisando <d>	Confirmada, Fechada, Em andamento, Aberta, Mudança pendente, Pesquisando, Resolvida
Cancelado	Fechado <d>	Fechado
Fechado		Confirmado, Aberto

Status atual	Transição padrão	Próximos status disponíveis
Fechado, sem resolução		Confirmado, fechado, aberto
Em espera		Confirmado, fechado, em andamento, aberto, mudança pendente, resolvido
Em andamento	Pesquisando <d>	Confirmado, aguardando resposta do usuário final, aguardando fornecedor, fechado, fechado sem resolução, aberto, mudança pendente, pesquisando, resolvido
Abrir	Confirmado <d>	Confirmada, Evitada pelo autoatendimento, Aguardando resposta do usuário final, Aguardando fornecedor, Fechada, Fechada não resolvida, Em andamento, Mudança pendente, Resolvida
Mudança pendente	Pesquisando <d>	Confirmada, Fechada, Em andamento, Aberta, Pesquisando, Resolvida
Pesquisando	Resolvido <d>	Fechada, Aberta, Resolvida, Aguardando resposta do usuário final, Fechada, Aberta

Fluxo de transição requisição de mudança

A tabela a seguir mostra o fluxo de transição requisição de mudança predefinido.

Status atual	Transição padrão	Próximos status disponíveis
Aprovação em andamento	Aprovado <d>	Aprovado, Cancelado, Fechado
Aprovado	Programado <d>	Cancelado, fechado, implementação em andamento, programado
Recuar		Aprovação em andamento, Fechada, Aberta, RFC
Cancelado		Fechado
Pausado pelo cliente		Cancelada, Fechada, Implementação em andamento, Rejeitada, Programada, Verificação em andamento
Em espera		Cancelado, fechado, implementação em andamento, programado
Implementação em andamento		Recuar, Cancelado, Fechado, Pausado pelo cliente, Rejeitado, Programado, Pausado pelo fornecedor, Verificação em andamento

Status atual	Transição padrão	Próximos status disponíveis
Abrir	RFC <d>	Aprovação em andamento, Cancelado, Fechado, Pausado pelo cliente, Implementação em andamento, Rejeitado, RFC, Programado, Pausado pelo fornecedor
Rejeitado	Fechado <d>	Aprovação em andamento, Cancelada, Fechada
RFC	Aprovação em andamento <d>	Aprovação em andamento, Cancelado, Fechado, Pausado pelo cliente, Implementação em andamento, Aberto, Rejeitado, Programado, Pausado pelo fornecedor
Programada	Implementação em andamento <d>	Cancelado, Fechado, Pausado pelo cliente, Implementação em andamento, Pausado pelo fornecedor, Verificação em andamento, Cancelado, Fechado, Implementação em andamento, Programado, Recuar, Fechado

Melhor prática: Transições de status predefinidas

As transições de status predefinidas entregues com o produto são Ativas em uma nova instalação e Inativas após a atualização. Para cada status relacionado na página Transitions List, há uma transição de status padrão (ou próximo status). O caminho adotado pela transição de status padrão reflete a melhor prática. As transições de status adicionais relacionadas na página Transitions List são fornecidas para preencher uma variedade de fluxos de trabalho de gerenciamento de ticket. No entanto, somente transições de status Ativas que usam essa melhor prática podem garantir que ocorra o fluxo de trabalho adequado para gerenciar Solicitações, Incidentes, Problemas e Requisições de mudança. Essa melhor prática ajuda a promover o movimento de tickets para resolução e fechamento dentro do ambiente de IT.

Por exemplo, as seguintes transições de incidente predefinidas listadas na página Lista de transições de incidente são definidas para Inativas para ajudar a promover a resolução e fechamento de incidentes:

Status	Novo status	Padrão	Status Description	Status do registro
Confirmada	Fechado	Não	Transição do status Confirmada para Fechado	Inativo
Confirmada	Fechado, sem resolução	Não	Transição do status Confirmada para Fechado, sem resolução	Inativo

Status	Novo status	Padrão	Status Description	Status do registro
Confirmada	Abrir	Sim	Transição do status Confirmada para Aberto	Inativo
Aguardando resposta do usuário final	Confirmada	Não	Transição do status Aguardando resposta do usuário final para Confirmada	Inativo
Aguardando resposta do usuário final	Abrir	Não	Transição do status Aguardando resposta do usuário final para Aberto	Inativo
Aguardando fornecedor	Confirmada	Não	Transição do status Aguardando fornecedor para Confirmada	Inativo
Aguardando fornecedor	Fechado	Não	Transição do status Aguardando fornecedor para Fechado	Inativo
Aguardando fornecedor	Abrir	Não	Transição do status Aguardando fornecedor para Aberto	Inativo
Fechado	Confirmada	Não	Transição do status Fechado para Confirmada	Inativo
Fechado, sem resolução	Confirmada	Não	Transição do status Fechado, sem resolução para Confirmada	Inativo
Fechado, sem resolução	Fechado	Não	Transição do status Fechado, sem resolução para Fechado	Inativo
Em espera	Confirmada	Não	Transição do status Em espera para Confirmada	Inativo
Em espera	Fechado	Não	Transição do status Em espera para Fechado	Inativo
Em espera	Abrir	Não	Transição do status Em espera para Aberto	Inativo
Em andamento	Confirmada	Não	Transição do status Em andamento para Confirmada	Inativo
Em andamento	Fechado	Não	Transição do status Em andamento para Fechado	Inativo
Em andamento	Abrir	Não	Transição do status Em andamento para Aberto	Inativo

Status	**Novo status**	**Padrão**	**Status Description**	**Status do registro**
Abrir	Fechado	Não	Transição do status Aberto para Fechado	Inativo
Mudança pendente	Confirmada	Não	Transição do status Mudança pendente para Confirmada	Inativo
Mudança pendente	Fechado	Não	Transição do status Mudança pendente para Fechado	Inativo
Mudança pendente	Abrir	Não	Transição do status Mudança pendente para Aberto	Inativo
Pesquisando	Abrir	Não	Transição do status Pesquisando para Aberto	Inativo

Transições de status para autoatendimento

Transições de status permitem controlar o movimento de um ticket de um estado discreto para outro (por exemplo, de Aberto para Fechado). Para funcionários usando o autoatendimento, é possível incluir botões nos formulários de Incidente e Solicitação para representar qualquer transição de status (na página 351).

Os botões de transição de status para fluxos de trabalho de processo de incidente e solicitação aparecem na interface do funcionário quando as transições de incidente ou solicitação estão vinculadas a tipos de transições ativas. Um tipo de transição define o texto do botão e controla o comportamento do formulário de detalhes do ticket. Quando são definidos botões, os botões herdados Fechar incidente (ou Solicitação) e Reabrir incidente (ou Solicitação) não são exibidos nos formulários de detalhe do ticket. Em vez disso, o funcionário pode alterar apenas o status do Incidente ou Solicitação usando os botões de transição de status configurados pelo administrador.

Por padrão, todos os tipos de transição predefinidos entregues com o produto estão inativos, assim os botões de transição de status não estão em vigor. Como administrador do sistema, você pode ativar e modificar tipos de transação predefinidos ou criar tipos de transição para acomodar seus fluxos de trabalho de transição de status. Após criar ou modificar um tipo de transação, você pode vinculá-los a qualquer transição de status de solicitação ou incidente.

Observação: para obter mais informações sobre tipos de transição, consulte a *Ajuda online*.

Mais informações:

Como as transições para autoatendimento funcionam (na página 363)
Como criar ou atualizar tipos de transição para transições (na página 364)
Como vincular tipos de transição a transações (na página 364)
Ativar tipos de transição predefinidos (na página 365)

Como as transições para autoatendimento funcionam

Tipos de transição e seus status correspondentes controlam quando os funcionários podem fechar e reabrir tickets como segue:

1. Tipos de transição ativos são vinculados a transições de status de incidentes (ou solicitações) pelo administrador.
2. O funcionário cria um incidente usando o autoatendimento.
3. O analista atribuído ao incidente descobre uma solução e passa o ticket para o status Resolvido.
4. Quando o ticket está no status Resolvido, o formulário de detalhes do funcionário exibe os botões de transição de status para Aceitar ou Rejeitar a resolução.
    - Se o funcionário aceitar a resolução, ocorre a transição de Resolvido para Fechado.
    - Se o funcionário rejeitar a resolução, ocorre a transição de Resolvido para Aberto.
5. Após o funcionário clicar em um botão, ele pode adicionar seus comentários no formulário de resolução que aparece.

Como criar ou atualizar tipos de transição para transições

Como administrador de sistema, você pode criar novos ou atualizar tipos de transição existentes e solicitar workflows de transição de status na página Lista de tipos de transição.

Para criar um tipo de transição para uma transição de status, faça o seguinte:

1. Na guia Administração, selecione Service Desk, Solicitação/Incidente/Problema, Tipos de transição.
2. Clique em Criar na página de lista.
3. Edite os campos conforme adequado na página de detalhes.

   O tipo de transição para a transição de status é criado.
4. Clique em Salvar.

   O novo tipo de transição aparece na Lista de tipos de transição quando você exibe a página novamente.

Para atualizar um tipo de transição, faça o seguinte:

1. Abra o tipo de transição desejado para edição na página Lista de tipos de transição.
2. Edite os campos conforme apropriado.
3. Clique em Salvar.

   O tipo de transição atualizado aparece na lista de Tipos de transição.

Como vincular tipos de transição a transações

Quando as transições de status estão vinculadas a tipos de transição, o formulário de detalhes do ticket do funcionário exibe botões de transição de status para Aceitar ou Rejeitar a resolução. Para vincular um tipo de transição a uma transição de status, faça o seguinte:

1. Na guia Administração, selecione Service Desk, Solicitações/incidentes/problemas, Transições de incidente (ou solicitação).
2. Abra a transição de status desejada para edição na página Request or Incident Transition List.
3. Especifique o tipo de transição desejado no campo Tipo de transição.
4. Clique em Salvar.

   O tipo de transição está vinculado à transição de status.

Ativar tipos de transição predefinidos

Por padrão, todos os tipos de transição predefinidos entregues com o produto estão inativos, assim os botões de transição de status não funcionando. Você pode ativar e modificar estes tipos de transição para acomodar seu fluxo de transição de status desejado.

Para ativar um tipo de transição predefinido:

1. Selecione Mostrar filtro na página Lista de tipos de transição.

   A parte superior da página revela campos de pesquisa adicionais.

2. Selecione Inativo no campo Status de registro e clique em Pesquisar.

   A Lista de tipos de transição exibe todos os tipos de transição inativos.

3. Clique com o botão direito do mouse no tipo de transição desejado e selecione Editar no menu.
4. Selecione Ativo no campo Status do registro.
5. Clique em Salvar, Fechar janela.
6. Clique em Pesquisar.

   A Lista de tipos de transição mostra o tipo de transição ativa.

Mais informações:

Tipos de transição predefinidos para Transições de status de incidentes (na página 365)
Tipos de transição predefinidos para Transições de status de Solicitação (na página 366)

Tipos de transição predefinidos para Transições de status de incidentes

A tabela a seguir descreve os tipos de transição predefinidos para transições de status de incidente:

Símbolo	Texto do botão	Texto do cabeçalho do formulário	Transição de status de incidente
Botão Aceitar resolução de incidente	Aceitar	Aceitar resolução	Resolvida para Fechada

Símbolo	Texto do botão	Texto do cabeçalho do formulário	Transição de status de incidente
Botão Rejeitar resolução do incidente	Rejeitar	Rejeitar resolução	Resolvida para Aberta
Botão Rejeitar fechamento de incidente	Solicitar fechamento	Solicitar fechamento	■ Para Fechado não resolvido de Aberto ■ Aguardando resposta do usuário final ■ Aguardando fornecedor ■ Em andamento ■ Confirmada

Tipos de transição predefinidos para Transições de status de Solicitação

A tabela a seguir descreve os tipos de transição predefinidos para transições de status de solicitação:

Observação: o status Encerramento solicitado para Solicitações é o equivalente do status Resolvido para Incidentes.

Símbolo	Texto do botão	Texto do cabeçalho do formulário	Transição de status de solicitação
Botão Aceitar resolução de solicitação	Aceitar	Aceitar resolução	Fechamento solicitado para Fechado
Botão Rejeitar resolução da solicitação	Rejeitar	Rejeitar resolução	Fechamento solicitado para Aberto

Símbolo	Texto do botão	Texto do cabeçalho do formulário	Transição de status de solicitação
Botão Solicitar fechamento de solicitação	Solicitar fechamento	Solicitar fechamento	■ Para Cancelado de Aberto ■ Aguardando resposta do usuário final ■ Aguardando fornecedor ■ Aprovação em andamento ■ Confirmada
Botão Fechar solicitação	Fechar	Solicitação fechada	De Em andamento para Fechado

Timers

Os timers agem como um cronômetro com vários limites que fornecem ao analista indicações do tempo decorrido. Você pode definir o período de tempo durante o qual o timer permanece em cada limite, e determinar que sua cor mude, que um alarme sonoro seja tocado ou que um lembrete seja exibido conforme cada limite seja alcançado. Um analista de service desk não pode controlar o cronômetro; apenas o administrador pode controlá-lo.

As solicitações são o único tipo de ticket que usa timers; portanto, defina timers para modelos combinados e internos de service desk.

Os seguintes valores de limite são predefinidos para o timer:

Duração do limite	Cor
00:00:00	Verde
00:01:00	Amarelo
00:05:00	Vermelho

Os valores predefinidos definem o início do cronômetro com a cor verde. Depois de um minuto, o timer exibe a cor amarela. Depois de 5 minutos, o timer exibe a cor vermelha. O tempo decorrido é exibido quando o analista exibe a solicitação em detalhes, e é redefinido sempre que uma nova solicitação é selecionada. Você pode adicionar etapas a esse processo ou alterar as etapas existentes.

Você pode marcar qualquer timer como ativo ou inativo. Quando marca um timer como inativo, ele não faz mais parte do processo, mas permanece disponível para uso futuro (isto é, não é excluído do banco de dados). Se você decidir usar o timer posteriormente, bastará marcá-lo como ativo.

Fusos horários

É possível definir fusos horários específicos para servidores, tipos de serviço, contatos e locais em seu sistema CA SDM. Você pode definir tipos de serviço locais, que se aplicam a um fuso horário específico, e tipos de serviço globais, que se aplicam a toda a empresa. Essas configurações eliminam a necessidade de o administrador saber o fuso horário de um servidor e ajustar manualmente os horários dos turnos de trabalho para adequação a diferentes fusos horários.

Mais informações:

Acionadores de evento de tipo de serviço (na página 368)
Acionadores de evento de fuso horário (na página 369)
Regras de fuso horário (na página 370)

Acionadores de evento de tipo de serviço

Tipos de serviço definem os eventos que são acionados após um tempo de espera especificado.

Exemplo: acionadores de evento por cronograma de turno de trabalho

Neste exemplo, um cronograma de turno de trabalho associado ao tipo de serviço restringe o tempo real em que um evento é acionado, como segue:

- O turno de trabalho é das 8:00 às 17:00.
- Atraso do evento de três horas
- O horário atual do servidor é 15:00.

O evento é acionado amanhã, às 9:00, horário do servidor, porque:

- De acordo com a hora atual do servidor, faltam duas horas para o turno de trabalho de hoje terminar (a hora atual é 15:00. O turno de trabalho termina às 17:00).
- O tempo de espera do evento é de três horas Duas horas desta espera são gastas no turno de trabalho do dia de hoje (15:00 às 17:00). Uma hora de espera adicional é levada para o turno de trabalho do próximo dia (8:00 às 9:00)

Consequentemente, o evento inicia às 9:00 do dia seguinte.

Acionadores de evento de fuso horário

Um fuso horário associado ao tipo de serviço pode impor os horários do acionador de evento.

Exemplo: acionadores de evento por fuso horário

Neste exemplo, um fuso horário associado ao tipo de serviço impõe o tempo real em que um evento é acionado, como segue:

- O turno de trabalho é das 8:00 às 17:00.
- Atraso do evento de três horas
- O horário atual do servidor é 15:00.
- O horário atual no fuso horário é 12:00.

O evento é acionado hoje, às 18:00, horário do servidor, porque:

- De acordo com a hora atual do servidor, faltam duas horas para o turno de trabalho de hoje terminar (a hora atual é 15:00. O turno de trabalho termina às 17:00).
- De acordo com a hora atual do fuso horário, faltam cinco horas para terminar o turno de trabalho de hoje (a hora atual é 12:00. O turno de trabalho termina às 17:00).
- O tempo de espera do evento é de três horas (12:00 às 15:00, hora do fuso horário. 15:00 às 18:00 hora do servidor).

Consequentemente, o evento inicia às 6:00, hora do servidor, ou 15:00, hora do fuso horário.

Regras de fuso horário

É possível especificar um fuso horário para um servidor, um local e um tipo de serviço. Também é possível dizer ao CA SDM para usar o fuso horário do Usuário final afetado de um ticket. O CA SDM usa as seguintes regras para determinar que fuso horário aciona um evento:

- **Fuso horário do usuário final afetado** — O CA SDM usa esta regra quando as seguintes condições existem:
  - A opção Usar fuso horário de usuário final é selecionada.
  - Um fuso horário é especificado para o usuário final afetado do ticket.
- **Fuso horário local do usuário final afetado** — O CA SDM usa esta regra quando as seguintes condições existem:
  - A opção Usar fuso horário de usuário final é selecionada.
  - Nenhum fuso horário é especificado para o usuário final afetado do ticket.
  - Um fuso horário é especificado para o local do usuário final afetado.
- **Fuso horário do tipo de serviço** — O CA SDM usa esta regra quando as seguintes condições existem:
  - Um fuso horário é especificado para o tipo de serviço.
  - A opção Usar fuso horário de usuário final não é selecionada.
- **Fuso horário do servidor** — O CA SDM usa esta regra quando as seguintes condições existem:
  - Um fuso horário é especificado para o servidor.
  - A opção Usar fuso horário de usuário final não é selecionada.
  - Nenhum fuso horário é especificado para o tipo de serviço.
- **Sem suporte para fuso horário** — O CA SDM usa esta regra quando as seguintes condições existem:
  - Nenhum fuso horário é especificado para o tipo de serviço.
  - A opção Usar fuso horário de usuário final não é selecionada.
  - Não há nenhum registro do servidor.

Anexos de arquivo

Às vezes você pode querer associar um arquivo a um ticket, como por exemplo no caso dos seguintes arquivos:

- Uma captura de tela de um determinado erro.
- Arquivos de log que levam a um problema.
- Um email que explica um problema.
- Um link da web que aponta para uma página da web que precisa de reparos.

Configure o service desk de modo que os usuários possam trabalhar com anexos. Todos os tipos de tickets podem ter anexos; portanto, configure anexos para todos os modelos de service desk.

O CA SDM classifica anexos como segue:

- Os anexos armazenados são carregados e armazenados em um repositório. Quando um analista revisa um anexo armazenado, o arquivo é recuperado usando um navegador e é exibido localmente. O arquivo armazenado permanece no repositório.

  Os anexos armazenados podem ser carregados a um repositório usando um servidor web que usa o protocolo HTTP. Utilizar um servidor web para armazenar arquivos permite o armazenamento e a recuperação usando a interface de usuário. Os repositórios de unidade compartilhada não podem ser acessados eficientemente usando um cliente web e, portanto, não têm suporte.
- Vinculado — Armazena somente um link para o arquivo no banco de dados.

Mais informações:

Fazer upload e download de anexos de arquivo (na página 372)
Repositórios (na página 372)

Fazer upload e download de anexos de arquivo

Todas as interfaces de cliente podem acessar os repositórios existentes para carregar e baixar anexos de arquivo, exceto:

- Repositórios de arquivo compartilhados podem ser acessados apenas quando o daemon de repositório está sendo executado em um computador com acesso ao arquivo compartilhado. O nome do servidor no registro do repositório (formulário de detalhes) deve ser um computador Windows que tenha acesso ao compartilhamento. Um daemon de repositório do CA SDM também deve estar sendo executado no computador.

  Observação: não há suporte para repositórios de unidade compartilhada no WIN2003.

- O download de arquivos .zip ocorre com base no momento em que eles são carregados. Os anexos de releases anteriores são baixados sem descompactação. Descompacte o arquivo no computador cliente. Os anexos carregados de uma interface cliente também são baixados sem descompactação. Isto é, o servidor descompacta o arquivo antes de retorná-lo, durante uma solicitação de download de cliente.

  Observação: os clientes legados continuam a funcionar do mesmo modo, e têm acesso imediato para novos uploads a repositórios existentes.

Observação: para obter informações sobre como trabalhar com anexos, consulte a *Ajuda online*.

Repositórios

Um repositório representa um diretório de disco em um computador local ou remoto. Você pode ter um repositório grande ou vários repositórios pequenos. A divisão dos repositórios é uma escolha determinada de acordo com suas práticas e necessidades comerciais.

Mover ou combinar os repositórios é simples porque todos os atributos de um repositório são definidos no registro do repositório. Apenas o repositório e o nome do arquivo são associados a cada ticket.

Os arquivos são carregados a um repositório e aí permanecem. Quando um arquivo é solicitado, ocorre uma das seguintes ações:

- Um navegador da web (HTTP) recupera e apresenta uma cópia do arquivo ao usuário.
- O aplicativo associado à extensão do arquivo abre o arquivo automaticamente.

Exemplo: alterar a estrutura de diretórios em um servidor web

Este exemplo mostra como alterar a estrutura de diretórios em um servidor web.

Altere o caminho de carregamento no registro do repositório.

Todos os anexos existentes apontam corretamente para o novo local automaticamente.

Configuração do repositório

É necessário configurar os repositórios para que os usuários do CA SDM possam trabalhar com anexos.

A arquitetura distribuída permite que uma localidade configure seus repositórios de acordo com suas necessidades. O servlet para um repositório não precisa residir no mesmo servidor dos arquivos vinculados. As localidades podem ter um servlet central para acessar todos os seus repositórios distribuídos ou um servlet dedicado para cada um de seus servidores de repositório.

Considere as configurações a seguir ao configurar repositórios:

- **Servidor de repositório em um servidor do CA SDM protegido** — Localidades que designam um servidor de repositório em um servidor do CA SDM protegido (geralmente um servidor secundário protegido por um firewall) não precisam expor o servlet nesse computador. Em vez disso, eles podem especificar um servlet que seja executado no servidor primário ou outro servidor de CA SDM sem restrições, e ainda assim carregar e baixar com êxito desse servidor. Dependendo da conexão em rede entre os dois servidores do CA SDM, pode haver impacto no desempenho ao carregar e baixar arquivos.

  Observação: uma boa maneira de configurar um repositório remoto é instalar um servidor secundário com o repositório no servidor remoto e definir o caminho de carregamento como um caminho local.

- **Servlet no mesmo servidor que o servidor de repositório** — Localidades que querem desempenho ótimo para carregar e baixar anexos, devem considerar esta configuração se o desempenho da rede for problemático e se arquivos muito grandes forem vinculados. Essa abordagem exige a exposição da porta do Tomcat (em geral, 8080) no servidor e deve ser observada se o computador estiver protegido por firewall.

Requisitos de sistema

Por padrão, os repositórios estão localizados no servidor primário, e nenhuma configuração extra é necessária para carregar anexos de arquivo. No entanto, ter o repositório em um computador remoto exige a instalação de um servidor secundário com o rep_daemon em execução no servidor primário: Os requisitos do sistema para o servidor são os seguintes:

- Servidor secundário (para acesso remoto) com um daemon de repositório sendo executado.
- Tomcat e servlet de carregamento

Para configurar um repositório em um computador remoto

1. Abra um prompt de comando e digite:

   cd $NX_ROOT/samples/pdmconf

2. Execute o pdm_edit.pl.

   Duas perguntas serão feitas. Responda a essas perguntas para retornar ao menu principal.

3. Selecione 8 e pressione Enter para selecionar Daemon de repositório.
4. Digite o nome do servidor secundário e pressione Enter.

   Observação: o nome do servidor secundário deve corresponder a NX_LOCAL_HOST no servidor secundário.

   O menu principal é exibido.

5. Selecione X e pressione Enter para salvar e sair.

   O arquivo salvo é o pdm_startup.rmt. Esse arquivo substitui o $NX_ROOT/pdmconf/pdm_startup.tpl.

6. Renomeie seu arquivo pdmconf/pdm_startup.tpl atual.
7. Copie seu novo arquivo pdm_startup.rmt para pdmconf/pdm_startup.tpl.
8. Instale um servidor secundário e inicie o proctor no servidor secundário.

   Observação: em sistemas Windows NT, o proctor é um serviço; em sistemas Linux, é um arquivo pdm_proctor_nxd.

9. Inicie o servidor primário e use pdm_status para verificar se o novo daemon é exibido.
10. Altere o nome do servidor e o caminho de carregamento para apontar para o computador remoto onde o daemon de repositório está sendo executado.

    O computador remoto é configurado para carregar anexos de arquivo.

Definir o repositório

Você deve definir um repositório usando a função administrativa da interface da web do CA SDM para usar anexos de arquivo.

Para definir o repositório

1. No menu Administração, selecione Anexos, Repositório para exibir a página Lista de repositórios.
2. Selecione Arquivo, Novo.

   A página Detalhes de Repositório aparece.
3. Digite dados nos seguintes campos:

   Símbolo

   Identifica o repositório com um nome como Somente arquivos grandes, Arquivos permanentes, etc.

   Repositório padrão

   Seleciona o repositório automaticamente para todos os anexos. Os usuários poderão alterar para um repositório diferente, se necessário.

   Nome do servidor

   Especifica o nome do servidor do repositório.

   Clique em Salvar.
4. Clique em OK.

   As páginas de detalhes e de lista fecham e a página principal aparece.

Anúncios

É possível usar o CA SDM para publicar anúncios para os usuários. Os anúncios ajudam a diminuir o número de chamados recebidos e promovem o aumento da produtividade por meio da resolução proativa de tickets e da comunicação de informações importantes a todos os usuários afetados. Os usuários podem percorrer os vários anúncios armazenados.

Observação: os anúncios podem ser usados em todos os modelos de central de serviços.

Você pode adicionar novos anúncios e atualizar os existentes. Os anúncios são parte da função de dados de referência do CA SDM, portando ao usar o tipo de acesso, é possível controlar quais contatos podem criar anúncios.

Um anúncio pode especificar um ou ambos dos seguintes itens:

Local

Especifica um local físico, por exemplo, uma cidade, um prédio ou um andar.

Organização

Especifica a ID de uma organização. Quando a organização é definida para um anúncio, apenas indivíduos atribuídos àquela organização podem visualizar o anúncio.

Quando o local ou a organização estão definidos para um anúncio, apenas contatos daquele local ou daquela organização podem recebê-lo. Qualquer contato pode ainda visualizar todos os anúncios que não sejam restritos por local ou organização. Por exemplo, se nenhum dos dois estiver definido, os contatos em todos os locais e organizações podem visualizar o anúncio.

Observação: você pode especificar anúncios usando a função administrativa da interface web. Para obter mais informações sobre como definir anúncios, consulte a *Ajuda online*.

Mais informações:

Visibilidade interna do anúncio (na página 377)
Especificar a urgência do anúncio (na página 377)

Visibilidade interna do anúncio

Você pode controlar se um anúncio é visível a usuários internos usando a caixa de seleção Interno na página Criar anúncio. A definição de Exibir logs internos do tipo de acesso do usuário conectado controla se um usuário pode exibir itens marcados como internos.

Especificar a urgência do anúncio

Você pode especificar a urgência de um registro do anúncio.

Para especificar a urgência do anúncio

1. Crie um anúncio ou navegue até a página Detalhes do anúncio para editar um anúncio existente.
2. Selecione um dos seguintes valores da lista suspensa Tipo de anúncio:

   Rotina

   Exibido em texto preto.

   Aconselhamento

   Exibido em texto laranja.

   Emergência

   Exibido em texto vermelho.

   Clique em Salvar.

   O registro do anúncio é codificado por cores na página Lista de anúncios.

Configuração de consultas armazenadas

O CA SDM oferece suporte ao uso de consultas armazenadas para produzir dois tipos de dados:

- Consultas ao gerenciador de filas permitem personalizar o Gerenciador de filas da interface da web adicionando campos de contagem para os itens que você quer.
- As consultas de KPI permitem recuperar informações históricas para um período especificado sobre o valor de uma contagem para uso na elaboração de relatórios com base na web.

As consultas armazenadas podem ser usadas em todos os modelos de service desk. as consultas armazenadas não têm por objetivo levar os usuários a uma nova página.

Os administradores definem as consultas armazenadas disponíveis aos usuários. Você pode modificar as consultas armazenadas predefinidas instaladas com o CA SDM ou definir suas próprias. É possível definir consultas armazenadas usando a função administrativa da interface da web.

Considere as informações a seguir sobre definições de consultas armazenadas:

- Uma cláusula de consulta armazenada válida é integrada em uma declaração SELECT apropriada e enviada ao mecanismo de DBMS subjacente para o processamento. Para desenvolver as declarações SELECT, consulte os arquivos de definição de objeto nos seguintes diretórios:
  - Windows: diretório-instalação\bopcfg\majic
  - UNIX: diretório $NX_ROOT/bopcfg/majic
- As consultas armazenadas usam declarações de objeto e atributos para criar a cláusula WHERE de SQL em vez dos nomes de campo no nível de banco de dados.
- O CA SDM não oferece suporte a uniões cartesianas de produto para consultas armazenadas Para ajudar a assegurar que sua consulta armazenada não produza uma união cartesiana, digite o comando apropriado ao seu sistema.
  - Windows: bop_cmd -f *diretório-instalação*\bopcfg\interp\bop_diag.frg "check_queries()"
  - UNIX: bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"

  Atualize as consultas resultantes para evitar uniões de produto cartesianas.
- A opção de URL de consulta armazenada é oferecida durante a criação de consultas armazenadas. A consulta armazenada de URL retorna resultados numéricos que só funcionam com o Gerenciamento de conhecimento.

Observação: para obter mais informações sobre a sintaxe de definição de objeto, consulte o *Guia de Referência Técnica*. Para obter mais informações sobre como definir consultas armazenadas, consulte a *Ajuda online*.

Números de sequência

Quando um ticket é aberto, o número de sequência seguinte disponível é automaticamente atribuído a ele. Por exemplo, se a última solicitação aberta for 5, o número seguinte a ser atribuído será o número 6.

Importante: Depois de instalar uma nova versão do CA SDM, a ID interna de registro para todos os tickets é redefinida como 1. Para ajudar a assegurar que IDs de registro duplicadas não sejam criadas, não crie tickets antes de restaurar todos os dados de backup.

Você pode personalizar como solicitações, requisições de mudança e ocorrências são numeradas ao incluir um prefixo ou sufixo exclusivo no esquema de numeração de cada um. Por exemplo, se quiser monitorar solicitações por mês, você poderá adicionar ao esquema de numeração de solicitação um identificador de mês como um prefixo ou sufixo.

Observação: para obter informações sobre como personalizar os números atribuídos aos tickets usando a função administrativa da interface web, consulte a *Ajuda online*.

Como um esquema de numeração separado é definido para cada tipo de ticket, configure esquemas de numeração para todos os modelos de service desk. Você pode controlar o formato da numeração de solicitações, requisições de mudança e ocorrências alterando as configurações de Número de sequência. Por padrão, novos tickets são numerados usando inteiros consecutivos. Como o campo de número de um ticket é, na verdade, um campo de sequência de caracteres e não numérico, você pode atribuir valores adicionais de sequência para usar como prefixo ou sufixos quando o número do ticket é gerado para um novo ticket. Por exemplo, você pode especificar r:, c:, e i: para prefixos de solicitações, requisições de mudança e incidentes. Essa configuração permite aos usuários diferenciar facilmente entre os vários tipos de tickets e evita confusões.

Incidentes e problemas compartilham esquemas de numeração com solicitações, pois incidentes e problemas são tipos de solicitação diferentes internamente.

Uso do log de auditoria

O CA SDM cria um log de auditoria que registra as seguintes informações:

- Todas as mudanças em uma ocorrência (Issue)
- Todas as mudanças em uma solicitação (Call_Req)
- Todas as mudanças em uma requisição de mudança (Change_Request)
- Todas as mudanças em tabelas de uma partição de dados (Domain)
- A ID de logon da pessoa associada à mudança e um dia/data/marca de data e hora associado
- Os valores anteriores e posteriores da atualização, inserção ou exclusão.
- A criação de contatos
- Atividades de criação e atualização do objeto nr

Observação: o log de auditoria captura modificações somente para o campo de partição de dados do contato, mas nenhuma outra atualização de registro do contato.

O recurso de log de auditoria é instalado automaticamente. Para ativá-lo, instale duas opções de log de auditoria com o Gerenciador de opções: audit_ins e audit_upd. Após instalar essas opções, você pode acessar o log de auditoria na guia Administração selecionando Service Desk, Lista de logs de auditoria. Você pode procurar a lista de logs de auditoria com uma ferramenta de pesquisa interna e usá-la para facilitar a geração de relatórios.

Observação: para obter informações sobre como instalar e definir valores para opções, consulte a *Ajuda online*.

Integração com o CA Network and Systems Management

Você pode definir registros de mensagem de gerenciamento de eventos e ações de registro de mensagem associadas no CA NSM para automaticamente criar solicitações, anexar comentários a solicitações existentes ou publicar anúncios no CA SDM.

Observação: para obter mais informações sobre a integração com o CA NSM, consulte o *Guia de Implementação*.

Capítulo 8: Controlando o comportamento do sistema

Esta seção contém os seguintes tópicos:

Uso do Gerenciador de opções (na página 381)
Como modificar o ambiente do sistema (na página 382)
Eventos (na página 383)
Macros (na página 383)

Uso do Gerenciador de opções

O CA SDM Web Client permite usar o Gerenciador de opções da guia Administrativo para fazer o seguinte:

- Definir opções
- Obtém uma lista de todas as opções disponíveis.
- Exibe um resumo de cada opção, como o aplicativo ao qual está associada, uma descrição breve e seu status.
- Exibir os detalhes de qualquer opção específica

  Ao exibir informações detalhadas sobre qualquer opção, você pode obter uma descrição completa de sua funcionalidade da *Ajuda online*. A descrição da *Ajuda online* inclui as ações especiais que você deve realizar ao alterar a opção. Por exemplo, depois de instalar ou desinstalar algumas opções, você deverá reciclar o servidor do CA SDM para que a opção tenha efeito. Se esse for o caso, a descrição da *Ajuda online* dessa opção descreverá essa ação.
- Revisar o status de todas as opções no nível de resumo
- Desinstalar qualquer uma das opções disponíveis

  Muitas das opções são pré-configuradas e instaladas durante a Instalação do CA SDM. Usar o Gerenciador de opções para instalar ou desinstalar opções pode alterar algumas as configurações padrão.
- Instalar qualquer opção definida

Observação: durante os ciclos de versões, algumas opções podem ser disponibilizadas por meio do suporte do CA SDM em resposta a solicitações de usuários. Para saber mais sobre essas opções, entre em contato com o suporte ao CA SDM. Para obter mais informações sobre como usar o Gerenciador de opções, consulte a *Ajuda online*.

Como modificar o ambiente do sistema

O CA SDM usa variáveis de ambiente especificadas no arquivo de modelo de ambiente (NX.env.tpl) para determinar certos comportamentos. É possível usar variáveis de ambiente para modificar alguns comportamentos do sistema. Em geral, o Gerenciador de opções é usado para controlar o comportamento do sistema, mas, às vezes, o Suporte Técnico da CA solicita que você modifique diretamente uma determinada variável de ambiente.

Considere o seguinte ao editar o arquivo de modelo de ambiente:

- As variáveis de ambiente definidas nesse arquivo podem ser substituídas ao definir a variável de ambiente no espaço de processo em que um processo é executado. Embora prática em alguns casos limitados, geralmente essa configuração não é recomendada. Preceder uma configuração variável com um arroba (@) evita que a variável seja substituída por outras variáveis durante o processo. A menos que haja uma razão específica para permitir uma substituição, o símbolo @ sempre precede o nome da variável no arquivo de modelo.
- Os caracteres de comentário para esse arquivo são # e !. O caractere ! também é usado para desativar uma opção.

Importante: Modifique o arquivo de modelo (NX.env.tpl) e permita que o processo de configuração aplique as mudanças ao arquivo de ambiente. Nunca modifique o arquivo de ambiente (NX.env) diretamente, inclusive em suas instalações de servidor secundário ou cliente.

Para modificar arquivo de modelo de ambiente

1. Faça o backup do arquivo de modelo de ambiente (.tpl) que corresponda ao ambiente de seu sistema.
   - UNIX — $NX_ROOT/pdmconf/NX.env.tpl.
   - Windows — diretório de -instalação\pdmconf\NX.env_nt.tpl.
2. Edite o arquivo de modelo de ambiente no servidor primário. É possível ver e modificar esse arquivo usando qualquer editor de texto (usuários do Windows usam o WordPad).

3. Faça as mudanças como instruído por seu técnico de suporte e salve as mudanças.
4. Execute o utilitário de configuração na instalação de servidor principal para aplicar as mudanças que você fez ao arquivo de modelo de ambiente no arquivo de ambiente real.

   Observação: para obter informações sobre como executar o utilitário de configuração, consulte o *Guia de implementação.*
5. Interrompa e reinicie o servidor primário do CA SDM para que as mudanças feitas no arquivo de ambiente entrem em vigor. Para evitar desativar o sistema, seu técnico de suporte pode instruí-lo a interromper e reinicializar apenas determinados processos, em vez de reciclar todo o servidor do CA SDM.

Eventos

É possível configurar eventos que estejam anexados a objetos para executar ações configuradas. Os eventos são procedimentos que são executados depois de um certo período de tempo. Por exemplo, um evento envia uma mensagem a um analista da central de serviços se uma ocorrência com "prioridade 1" não for resolvida em uma hora. Outras partes do sistema usam eventos, por exemplo, Tipos de serviço.

É possível definir eventos para solicitações, incidentes, problemas, requisições de mudança, ocorrências, contatos, itens de configuração e inquilinos globais e específicos. O CA SDM programa o tempo de execução dos eventos com base no tempo de espera e turno de trabalho.

Observação: para obter mais informações sobre eventos, consulte a *Ajuda online*.

Macros

As macros são pequenos scripts que definem quaisquer condições ou ações. Quando Eventos ou Comportamentos são executados, eles podem executar uma ou mais macros de Ação. Para que as macros possam ser executadas, uma macro condicional pode ser usada para determinar o conjunto de macros de Ação a ser executado.

As macros podem ser usadas nas seguintes situações:

- Eventos
- Modelos de comportamento de ocorrência ou mudança
- Notificações de atividade

O produto inclui várias macros. Os usuários podem criar tipos adicionais.

Observação: os clientes não podem adicionar macros de Ação ou Condição, mas podem criar condicionais simples com condições definidas pelo local. As condições definidas pelo local são macros não complexas que podem ser criadas em caixas de diálogos da GUI; elas não substituem as macros do tipo Condição.

Para cada macro, você deve especificar o tipo de objeto que deseja que a macro use. Se desejar criar uma condicional definida pelo local para verificar os valores de uma solicitação, você deverá definir o tipo como Solicitação. Quando você seleciona macros para Eventos e Comportamentos, o CA SDM exibe apenas macros com um tipo que corresponda ao tipo no Evento ou Comportamento.

Tipos de macro

Cada uma das macros a seguir possui um tipo específico que descreve seu uso:

Ação

Executa algum tipo de ação, como aumentar a prioridade em uma ocorrência.

Anexar evento

Anexa um objeto de Evento a um Item Configuração, Contato, Solicitação, Ocorrência ou Mudança.

Condição

Avalia algumas condicionais verdadeiro ou falso.

Executa uma Ação do CA IT PAM

Executa uma ação do CA IT PAM. O CA IT PAM é um mecanismo de fluxo de trabalho que ativa o gerenciamento e a geração de relatórios em grupos de tarefas que podem exigir aprovações eletrônicas.

Executa uma Ação do CA Workflow

Executa uma ação do CA Workflow O CA Workflow permite gerenciar processos de fluxo de trabalho em seu ambiente, tais como atividades de acompanhamento que são concluídas em tickets associados a uma área ou categoria específica.

Referência remota

Executa um programa externo no servidor.

Notificação múltipla

Envia uma notificação a um ou mais contatos. Esse tipo de macro é especialmente útil, uma vez que é possível especificar a mensagem, os destinatários e o nível de urgência.

Condição Site-Defined

Cria eventos com base em condicionais verdadeiro ou falso, com base em atributos do ticket para reforçar níveis de serviço. Por exemplo, é possível criar uma macro Condição que avalie como verdadeiro se uma Solicitação é prioridade 1 e ainda não está atribuída. É possível anexar a condição a um Evento que executa assim que uma solicitação é criada.

Usar macros com eventos

Em um detalhe de Evento, você pode opcionalmente especificar uma macro condicional para o campo Condição de evento. Você também pode especificar qualquer número de macros (exceto condicionais) em Executar em colunas Verdadeiro e Falso. Quando o evento é ativado, a macro condicional é primeiro avaliada. Se ela for verdadeira, todas as macros na coluna Verdadeiro serão ativadas. Se ela for falsa, todas as macros na coluna Falso serão ativadas. A macro condicional também pode verificar se o Destinatário foi definido, o nível de prioridade, a violação de tipo de serviço e assim por diante. Se nenhuma macro de Condição de evento for especificada, o evento executa automaticamente as macros Verdadeiras.

Em um detalhe de Evento, você pode selecionar entre vários tipos de macros para notificar contatos, definir valores no objeto de contexto, executar uma referência remota ou anexar outro evento.

Usar macros no comportamento de ocorrências e categorias de mudança

Você também pode usar macros no comportamento de ocorrências e categorias de mudança. Em um detalhe de Categoria, você pode examinar a guia Fluxo de trabalho e selecionar um status de fluxo de trabalho. Nos detalhes do fluxo de trabalho, clique no botão de Comportamento. De modo similar a um evento, você pode definir uma condição e ações resultantes.

Na guia Transição dos detalhes de comportamento, você pode especificar uma macro do tipo condicional para determinar se a tarefa pode mudar de status. Isso é ativado quando um usuário tenta alterar o status da tarefa desse valor a um diferente. Se a condição for falsa, a atualização de status não será permitida.

Tarefas de fluxo de trabalho reais são criadas a partir dos modelos no modelo de categoria. Quando o valor de status de uma tarefa é alterado e salvo, o comportamento especificado no modelo de categoria é ativado; isso significa que a condição e as ações resultantes são executadas.

Observação: use uma macro Anexar evento para anexar um evento a uma tarefa de fluxo de trabalho.

Usar macros com notificação múltipla

Notificação múltipla

O corpo da mensagem da notificação múltipla aponta diretamente para a tabela do objeto selecionado. Assim, quando fizer referência a campos na tabela de objeto, (por exemplo, CR (Call_Req)), você poderá fazer referência ao nome de atributo do campo. Se desejar especificar as informações de descrição do ticket de Solicitação de chamada, você poderá digitar o seguinte no corpo da mensagem:

```
Descrição: @{description}
```

Uma QREL (Relação de consulta) é uma relação que contém uma lista de objetos definidos por uma cláusula do tipo WHERE do SQL. É possível adicionar a QREL à descrição de uma macro de notificação múltipla. Se quisesse colocar a QREL na descrição para act_log QREL <-- alg, poderia usar o seguinte em uma macro de notificação:

```
@{act_log.0.description}
```

É possível usar variáveis de substituição para tornar mensagens de notificação mais relevantes e dinâmicas. Essas variáveis de substituição tem o formato @{caminho_atributo_aqui}, onde caminho_atributo_aqui é um atributo de algum objeto do CA SDM. Quando a notificação é enviada, a variável é substituída pelo valor de atributo especificado.

Uma notificação (seja de um log de atividades ou uma notificação múltipla) sempre tem algum contexto de base (um ponto de referência), que é normalmente um ticket ou uma tarefa de fluxo de trabalho Em notificação múltipla, o campo tipo de macro da Notificação especifica o objeto base. Você pode usar a sintaxe @{} para fazer referência a qualquer atributo nesse objeto.

Exemplo: uma Notificação múltipla do tipo Solicitação pode fazer referência a qualquer atributo no objeto 'cr' (Call_Req). Para incluir a descrição de Solicitação, especifique @{description} (a notação de ponto é usada para seguir referências a outros objetos). Por exemplo, para incluir o sobrenome do responsável pela Solicitação: @{assignee.last_name}.

Usar macros com condições definidas pelo local

Condição Site-Defined

A macro Condicional é composta de uma ou mais condições *atômicas*. Cada átomo testa o valor de um único atributo. Portanto, se quiser definir a condição com base nos valores para Responsável e Categoria, a macro Condicional provavelmente usará dois átomos, um para Responsável e um para Categoria. Quando você usa uma Macro Condicional em um evento, os átomos individuais são ligados por um operador booleano, em geral ‘E' ou ‘OU'.

Os Detalhes da macro condicional mostram uma lista de átomos, que é lida da esquerda para a direita como se segue:

Atributo	Operador	Valor	Lógico	Conversão
Responsável	Igual a	Jones	E	O destinatário é Jones e...
Custo	Menor que	600	OU	O custo é um valor de número inteiro menor que 600 ou...
Grupo	Empty/NULL		E	O campo Grupo está vazio.

Observação: conectores lógicos (AND, OR) conectam dois átomos. Quando você tem dois átomos, como um e dois, eles são ligados pelo conector do átomo um. O conector do átomo dois não é usado. Além disso, algumas seleções de Operador não são úteis, como quando um atributo é um *Destinatário* e você usa o operador *Menor que* — isso não faria sentido. Para obter mais informações sobre a configuração de macros condicionais, consulte a *Ajuda online*.

Capítulo 9: Configurando a interface da Web

Esta seção contém os seguintes tópicos:

Configuração da interface da Web (na página 389)
Como a interface da web funciona (na página 389)
Web Director e distribuição de carga da web (na página 390)
Configuração de web directors e de mecanismos da web (na página 396)
Melhorar o desempenho com o armazenamento em cache no navegador (na página 428)
Registrar o comportamento de bloqueio na interface da Web (na página 431)
Imprimir páginas da Web do CA SDM (na página 432)
Modificação de arquivo de configuração (na página 432)

Configuração da interface da Web

A *interface da web* fornece ao CA SDM funcionalidade pela internet. A interface da web ativa a procura independente da base de conhecimento, reduzindo o número de chamadas ao service desk e acelerando o tempo de resolução. A interface também permite fazer o seguinte:

- Abrir, processar e fechar tickets
- Exibir e publicar anúncios
- Acessar dados de suporte

Depois de instalado e configurado o CA SDM de acordo com as instruções no *Guia de Implementação*, você poderá administrar e proteger o CA SDM, além de configurá-lo para atender às suas necessidades. Você configura a segurança da interface da Web por meio do uso de funções e tipos de acesso. Você pode personalizar a interface para usá-la com navegadores da web.

Como a interface da web funciona

A interface da Web do CA SDM usa um servidor HTTP padrão, como o Tomcat, Apache ou o Microsoft IIS (Internet Information Server).

- Com o servidor Tomcat, um Java Servlet, pdmweb.jar, processa solicitações da web.
- Com o Apache ou o servidor de IIS, uma interface de CGI, pdmweb.exe, processa solicitações da web.

A interface da web do CA SDM funciona como segue:

1. Quando um usuário solicita uma página da web do CA SDM, o servidor HTTP chama o pdmweb.jar ou pdmweb.exe, que estabelece uma conexão com um daemon (ou Windows Service) do CA SDM chamado mecanismo da web.
2. O mecanismo da web interpreta a solicitação do usuário. A maioria das solicitações exige que o mecanismo da Web procure um arquivo de modelo HTML (HTMPL) e converta-o em HTML padrão.
3. Normalmente, o processo de conversão exige que o mecanismo da Web comunique-se com um servidor do CA SDM para ler ou atualizar o banco de dados e inclua informações do banco de dados no HTML gerado.
4. Uma vez concluído o HTML, o mecanismo da web o envia ao pdmweb.jar ou pdmweb.exe que, por sua vez, o envia ao navegador do usuário.
5. Depois que os dados forem enviados ao navegador, o pdmweb.exe é finalizado, porém o pdmweb.jar permanece ativo.

Web Director e distribuição de carga da web

À medida que o uso da web aumentar em sua localidade, poderá ser útil distribuir a carga de trabalho entre vários mecanismos da web, servidores HTTP ou ambos. A distribuição permite aumentar a capacidade do servidor web de acordo com o nível de uso exigido por sua organização. Você pode usar o Web Director, fornecido com o CA SDM, para distribuir a carga da web. O Web Director recebe solicitações de conexão de usuários, seleciona um mecanismo da web para lidar com a solicitação e redireciona a solicitação a esse mecanismo da web. Com exceção da mudança de URL, esse processo é invisível ao usuário final, que sempre acessa o CA SDM usando o mesmo URL, qualquer que seja o número de mecanismos da Web configurados.

Você pode usar o Web Director das seguintes maneiras:

- Para configurar o CA SDM para o uso eficiente dos soquetes de segurança (SSL).

  O protocolo HTTPS permite que transações da Web sejam criptografadas, fornecendo segurança máxima para dados confidenciais, especialmente senhas. No entanto, as páginas que usam SSL não podem ser incluídas em cache, o que pode ter um impacto negativo no desempenho.

- Para direcionar logons a um mecanismo da web específico.

  Depois que um usuário for autenticado, o Web Director poderá mover a sessão para um mecanismo da web diferente, que pode estar em um servidor HTTP diferente. Isso permite configurar o SSL para um mecanismo da web de logon, fornecendo proteção máxima para suas senhas ao mesmo tempo em que usa um protocolo HTTP padrão para outras transações e aumentando seu desempenho.

- Para ter vários web directors, cada um lidando com um grupo de mecanismos da web diferentes.

  Essa configuração pode ser útil em organizações geograficamente distribuídas que desejam posicionar grupos de mecanismos da web mais próximos fisicamente de seus usuários finais.

Web.cfg e CA SDM

Você pode usar o script pdm_edit.pl fornecido para ajudá-lo a configurar mecanismos da Web do CA SDM. Sem o script, um usuário que adicione um mecanismo da Web manualmente deverá especificar o nome e criar uma instância exclusiva de um arquivo web cfg. O script executa estas tarefas automaticamente.

Quando você usa o script pdm_edit.pl para configurar um mecanismo da Web, ele cria e nomeia um script automaticamente. O nome é criado da seguinte maneira:

“*<Host_Name>*`-web[#].cfg`”

nome do host

Especifica o servidor como primário, quando o mecanismo da web reside em um servidor primário; ou especifica o nome do host do servidor real, quando o mecanismo da web reside em um servidor secundário.

[#]

Especifica um valor de número inteiro atribuído automaticamente por pdm_edit.pl e incrementado de acordo com cada mecanismo da web em um servidor.

No caso do arquivo de configuração do mecanismo da web padrão, a instalação do CA SDM fornece um arquivo de configuração de mecanismo da web padrão, definido pelo seguinte arquivo:

```
$NX_ROOT/bopcfg/www/web.cfg
```

Após o mecanismo da Web padrão ser modificado por meio do pdm_edit.pl, o arquivo de configuração de mecanismo da Web que é gerado segue esse novo esquema de nomenclatura:

```
<Host_Name>-web[#].cfg
```

Daí em diante, o arquivo web.cfg original, com todas as suas personalizações, será ignorado. Se o usuário desejar manter as personalizações do arquivo web.cfg original, deverá verificar se $NX_ROOT/bopcfg/www/web.cfg está selecionado como o arquivo de modelo a ser usado quando o pdm_edit.pl criar arquivos <*Host_Name*>-web[#].cfg.

Atribuir um mecanismo da Web a um WebDirector

Um mecanismo da Web é atribuído a um Web Director por meio dos parâmetros do WebDirector no seguinte arquivo de mecanismos da Web:

```
‘<Nome_host>-web[#].cfg'
```

Observe que, embora cada mecanismo da Web exija seu próprio arquivo <Host_Name>-web[#].cfg, os Web Directors não usam um arquivo de configuração da Web. Essa atribuição de mecanismo da Web/Web Director é inicialmente realizada usando o seguinte script de utilitário:

```
'pdm_edit.pl'
```

Podem ser necessárias mudanças adicionais aos parâmetros de ‘webdirector' do <Nome_host>-web[#].cfg do mecanismo da Web para modificar ainda mais o comportamento de redirecionamento de mecanismos da Web. Se um mecanismo da Web não for atribuído a um Web Director (o padrão), o parâmetro Usedirector do arquivo de configuração do mecanismo da Web será definido como No. O CA SDM vai ignorar os parâmetros de ‘webdirector' restantes do mecanismo da Web.

Após a atribuição de um mecanismo da Web a um Web Director, os seguintes parâmetros definem como o mecanismo da Web interage com o Web Director a ele atribuído:

- UseDirector Yes | No | AfterLogin | BeforeLogin
- WebdirectorSlumpName ("slump name" é automaticamente atribuído)
- O WillingnessValue varia de ‘0' a ‘10'
- RedirectingURL [http/https]://<nome_computador>/<diretório cgi>/<nome cgi>

Defina a função do mecanismo da Web com parâmetros do Web Director

Após configurar um mecanismo da Web para que use um Web Director, o mecanismo da Web assume uma função específica. Essa função define que solicitações do Web Client serão tratadas pelo mecanismo da Web. As funções são as seguintes:

- Aceitar apenas logon (redireciona não-logon para outro local)
- Aceitar apenas solicitação sem logon (redireciona logons para outro local)
- Aceitar solicitações de logon e sem logon (mecanismo da Web para 'propósitos gerais')

Essa função é determinada pelos valores de parâmetros do 'WebDirector' no arquivo '<Nome_host>-web[#].cfg' do mecanismo da Web. A tabela a seguir ilustra a relação entre a função do mecanismo da Web e a configuração dos parâmetros do Web Director:

Função do mecanismo da Web	Configurações de parâmetros do 'webdirector' no '<Nome_host>-web[#].cfg'
Aceitar solicitações de logon	'UseDirector AfterLogin'; 'Willingness 0'
Aceitar atividade sem logon	'UseDirector BeforeLogin'; 'Willingness [1 a 10]'
Propósito geral	'UseDirector Yes'; Willingness [1-10]'

Ambiente sem SSL com equilíbrio de carga de trabalho básico

Você pode usar o web director em um ambiente não-SSL com equilíbrio de carga básico. O web director equilibra a carga em todos os mecanismos da web de acordo com o valor de disposição de cada mecanismo. Cada mecanismo da web pode atender solicitações de logon e não-logon. O protocolo HTTP é usado para comunicação entre o cliente web e o servidor web.

Para cada mecanismo da web sob o controle do web director, defina os parâmetros do web director em ‘<*Host_Name*>-web[*#*].cfg’ do mecanismo da web da seguinte maneira:

- UseDirector Yes
- WebDirectorSlumpName (não altere este valor)
- WillingnessValue [1 a 10]
- RedirectingURL (o valor de protocolo anexado como prefixo pode estar ausente ou ser ‘http')

Ambiente com SSL global com equilíbrio de carga de trabalho básico

Você pode usar o web director em um ambiente SSL global com equilíbrio de carga básico. O web director equilibra a carga em todos os mecanismos da web de acordo com o valor de disposição de cada mecanismo. Cada mecanismo da web pode atender solicitações de logon e não-logon. O protocolo HTTPS deve ser usado em todos os tipos de comunicação entre o Web Client e o servidor da Web.

Para cada mecanismo da web sob o controle do web director, defina os parâmetros do web director em ‘<*Host_Name*>-web[*#*].cfg’ do mecanismo da web da seguinte maneira:

- UseDirector Yes
- WebDirectorSlumpName (não altere este valor)
- WillingnessValue [1 a 10]
- RedirectingURL (o valor de protocolo anexado como prefixo deve ser ‘https’)

logon direcionado em um ambiente sem SSL com equilíbrio de carga de trabalho opcional

Você pode usar o web director para um logon direcionado em um ambiente não-SSL com equilíbrio de carga opcional. O mecanismo da web do tipo "apenas logon" atende apenas as solicitações de logon. Os mecanismos da web restantes sob controle do web director atendem todas as outras solicitações. Essa configuração encaminha toda a carga de trabalho de solicitações de logon aos mecanismos da web do tipo apenas logon especificados. O protocolo HTTP é usado para a comunicação entre o Web Client e o servidor da Web.

No caso de mecanismos da web do tipo apenas logon, defina os parâmetros do web director no arquivo '<*Host_Name*>-web[*#*].cfg' do mecanismo da web da seguinte forma:

- UseDirector AfterLogin
- WebDirectorSlumpName (não altere este valor)
- WillingnessValue 0
- RedirectingURL (o valor de protocolo adicionado como prefixo pode estar ausente ou ser 'http')

No caso de mecanismos da web do tipo não-logon, defina os parâmetros do web director no arquivo '<*Host_Name*>-web[*#*].cfg' do mecanismo da web da seguinte forma:

- UseDirector BeforeLogin
- WebDirectorSlumpName (não altere este valor)
- WillingnessValue [1 a 10]
- RedirectingURL (o valor de protocolo anexado como prefixo pode estar ausente ou ser 'http')

Logon SSL direcionado em ambiente misto com equilíbrio de carga de trabalho opcional

Você pode usar o web director para um logon SSL direcionado em um ambiente web misto SSL/não-SSL com equilíbrio de carga opcional. Todas as solicitações de logon da web são redirecionadas a mecanismos da web SSL, nos quais são processadas. Todas as outras solicitações são redirecionadas a mecanismos da web não-SSL, nos quais são processadas. O protocolo HTTPS deve ser usado em todos os tipos de comunicação entre o Web Client e o mecanismo da Web SSL.

Configuração de web directors e de mecanismos da web

Familiarize-se com as seguintes informações para adicionar e configurar web directors e mecanismos da web, com base no servidor e em tipos de componente:

SSL

Especifica o protocolo SSL (Secure Socket Layer).

pdm_edit.pl

Especifica o script Perl do CA SDM usado para adicionar e modificar mecanismos da web, web directors, gerenciadores de objetos e outros componentes.

CGI I/F

Especifica o nome do script para os mecanismos da web e web directors atribuídos por pdm_edit.pl. Esse valor é o nome de um CGI real executável quando o IIS ou o Apache é usado como servidor HTTP; é um parâmetro de servlet quando o Tomcat é usado como servidor HTTP.

Exemplos: (mecanismos da web) pdmweb1, pdmweb2, (web directors) pdmweb_d1 e pdmweb_d2

Os sistemas que usam servidores servlet como o Tomcat não necessitam de executáveis CGI/IF. O CGI/IF é simulado por uma execução de servlet no servidor servlet, em vez disso, estes sistemas exigem um arquivo web.xml no diretório: $NX_ROOT/bopcfg/CATALINA_BASE/webapps/CAisd/WEB-INF

Pdm_edit.pl cria arquivos de web.xml de exemplo que são denominados <*hostname*>-web.xml.tpl. Copie esses arquivos para o servidor apropriado no diretório WEB-INF para que eles substituam o arquivo web.xml.tpl em cada servidor, depois reconfigure o servidor secundário.

Logon SSL

Especifica a configuração de CA SDM na qual um ou mais mecanismos da web residem em um diretório virtual protegido por SSL e lidam exclusivamente com as solicitações de logon no cliente web usando a comunicação HTTP criptografada. Depois que a autenticação de usuário é concluída, um web director redireciona o cliente web a um mecanismo da web qualificado, que reside em um diretório virtual não imposto por SSL para o restante da sessão do cliente, usando comunicação HTTP sem criptografia.

Mecanismo da web de logon seguro

Especifica o mecanismo da web no ambiente de Logon SSL que lida exclusivamente com as solicitações de autenticação de usuário de cliente web do CA SDM.

Mecanismo da web não seguro

Especifica o mecanismo da web no ambiente de Logon SSL que lida com todas as solicitações de autenticação que venham de não-usuários do cliente web depois da autenticação do usuário pelo mecanismo da web de logon seguro.

Função do mecanismo da web

Especifica as tarefas de um mecanismo da web após ser atribuído a um web director. Essas funções incluem:

- Processar apenas solicitações de logon do cliente web.
- Processar tudo, exceto as solicitações de logon do cliente web.
- Processar todas as solicitações do cliente web.

Mais informações:

Como implementar um ambiente de logon SSL com somente um servidor primário (na página 397)
Configuração do servidor (na página 407)
Mecanismos da Web (na página 415)

Como implementar um ambiente de logon SSL com somente um servidor primário

Você pode implementar um ambiente de logon SSL com somente um servidor primário.

Observação: o servidor primário deve ser instalado e configurado para criar o sistema.

Para implementar um ambiente de logon SSL, faça o seguinte:

1. Verifique se servidor da web com SSL importou com êxito um certificado SSL.
2. Crie uma cópia (incluindo subdiretórios) do diretório ‘$NX_ROOT/bopcfg/www/wwwroot' e atribua a ele o seguinte nome:

   ‘$NX_ROOT/bopcfg/www/wwwrootsec’

3. Adicione um novo diretório virtual ao servidor web chamado *CAisdsec*. Aponte esse diretório virtual para o seguinte diretório físico:

   '$NX_ROOT/bopcfg/www/wwwrootsec'

   Verifique se as permissões do diretório virtual para CAisdsec correspondem às permissões do diretório virtual CAisd para execução de scripts. Ative o SSL para o diretório virtual CAisdsec.

   Observação: neste exemplo, CAisdsec é definido pelo usuário e pode ser renomeado.

4. Crie um sistema somente com um servidor primário.

Como criar um sistema somente com um servidor primário

Você pode criar um sistema que usa apenas um servidor primário.

Observação: o servidor primário deve ser instalado e configurado para criar o sistema.

Para criar um sistema somente com um servidor primário, faça o seguinte:

1. Usando pdm_edit.pl adicione e/ou edite entradas de webdirector, como preferir. Um web director pode distribuir a carga entre vários mecanismos da web. Atribua todos os novos mecanismos da web e web directors ao host denominado primário. Esse host é o servidor primário.

   Observação: a atribuição automática de CGI I/F do web director atribui nomes dentro do pdm_edit.pl:

   - Ao primeiro web director no servidor primário é automaticamente atribuído o nome pdmweb_d1.exe.
   - O segundo web director no servidor primário será nomeado como pdmweb_d2.exe.
   - O terceiro seria nomeado como pdmweb_d3.exe, e assim por diante.

   Um servidor secundário também pode ter web directors com os valores de CGI I/F pdmweb_d1.exe, pdmweb_d2.exe e pdmweb_d3.exe. Não há conflito de nome porque os nomes de web directors são exclusivos para o computador local em que os web directors estão sendo executados.

2. Leia as seguintes informações que podem se aplicar, dependendo de seu ambiente de mecanismo da web do CA SDM:

   - Número de mecanismos da web a adicionar — Durante a implementação de qualquer esquema de equilíbrio de carga de mecanismo da web, Logon SSL, ou ambos, ao menos dois mecanismos da web devem ser atribuídos ao mesmo web director.

   - Ambiente de logon SSL — Quando você definir o mecanismo da web de logon seguro em pdm_edit.pl, este mecanismo da web deve estar sob o controle de um web director. Defina o valor de parâmetro de protocolo do mecanismo da web de logon seguro como https para assegurar que o web director crie o valor do URL de redirecionamento para o cliente web.

3. Salve as mudanças e saia do script pdm_edit.pl, especificando que arquivo usar para um modelo do web.cfg quando solicitado.

   Observação: Webdirectors não usam um arquivo ‘<Host_Name>-web[#].cfg’. No entanto, mecanismos da Web exigem um arquivo ‘<Nome_host>-web[#].cfg’ exclusivo. Os arquivos web.cfg de exemplo são automaticamente gerados usando o script pdm_edit.pl ao salvar e sair do script. O usuário é solicitado a especificar um arquivo web.cfg a ser usado como modelo na criação dos arquivos de configuração da web. As personalizações no arquivo web.cfg original podem ser importadas para os novos arquivos de configuração da Web especificando o web.cfg original como o arquivo desejado de modelo.

4. Copie e salve os seguintes arquivos, uma vez que ter um backup desses arquivos é útil sempre que você decidir restaurar o ambiente original:

   - $NX_ROOT/pdmconf/pdm_startup.tpl

   - $NX_ROOT/pdmconf/pdm_startup

   - Arquivo $NX_ROOT/bopcfg/www/web.cfg

   - Qualquer arquivo primary-web[#].cfg existente

   - $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml e web.xml.tpl

5. Mova $NX_ROOT/samples/pdmconf/pdm_startup.rmt para $NX_ROOT/pdmconf e renomeie-o como pdm_startup.tpl.

6. Para cada mecanismo da Web que foi atribuído a um Webdirector, certifique-se de que os parâmetros do “webdirector” de ‘<Nome_do_host>-web[#].cfg’ foram definidos corretamente examinando o arquivo em um editor de texto. Se necessário, modifique o parâmetro ‘webdirector' para refletir a função do mecanismo da web que você quer. Em seguida, copie-os para o diretório: $NX_ROOT/bopcfg/www.

7. Mova todos os arquivos $NX_ROOT/samples/pdmconf/primary-web[#].cfg para o diretório $NX_ROOT/bopcfg/www.

8. Se você estiver usando um servidor servlet como o Tomcat, o utilitário pdm_edit.pl cria arquivos web.xml.tpl que podem substituir o arquivo web.xml.tpl em cada servidor que hospeda um mecanismo da web. Esses arquivos são nomeados primary-web.xml.tpl. Renomeie os arquivos e copie-os para o diretório: $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF.

   Se estiver usando um servidor HTTP como IIS ou Apache, crie cópias do ‘pdmweb.exe’ no diretório $NX_ROOT/bopcfg/www/wwwroot, um ‘pdmweb[#].exe’ para cada mecanismo da Web e um ‘pdmweb_d[#].exe’ para cada webdirector definido em pdm_edit.pl. Verifique se ‘pdmweb[#].exe’ e ‘pdmweb_d[#].exe’ foram nomeados de acordo com os valores de CGI I/F corretos das definições de script de pdm_edit.pl (por exemplo: ‘pdmweb1.exe', ‘pdmweb2.exe', pdmweb_d1.exe' etc.)

9. Se você estiver usando o IIS e quiser adicionar extensões de servidor para cada interface CGI, poderá copiar o arquivo primary-site.dat para o diretório $NX_ROOT/bopcfg/www como site.dat. Quando o sistema é reconfigurado, essas localidades são adicionadas ao IIS.

10. Reconfigure o servidor primário sem reinicializar o banco de dados e iniciar serviços.

11. Após a reconfiguração, verifique se as configurações atuais são válidas. Inicie os daemons do CA SDM. Verifique se não há erros nos arquivos de stdlog. Use o pdm_status para exibir os daemons e seu status. Em um navegador, você pode acessar o sistema: http://localhost:8080/CAisd/pdmweb.exe.

12. Para uma integração do Gerenciamento de conhecimento com CA SDM, se o SSL tiver sido imposto para CA SDM, o valor de protocolo do URL do CA SDM deve ser alterado.
    a. Em Gerenciador de configurações do Knowledge Tools, Geral, Integração, altere o valor de protocolo do URL do CA SDM de http para https.
    b. Salve e saia.
13. Abra um navegador da web na página de logon do CA SDM e verifique se um usuário pode efetuar logon e se logon/redirecionamento está adotando o comportamento esperado.

Verificar os valores de parâmetros do web director

Você pode verificar os valores de parâmetros do web director

Para verificar os valores de parâmetro

1. No caso de mecanismos da web de logon seguro, edite <*Host_Name*>-web[#].cfg, como segue:
    a. Mude o valor do parâmetro de CAisd de /CAisd para /CAisdsec.
    b. Altere o valor do parâmetro UseDirector de Yes para AfterLogin se o web director usa passar pela autenticação.
    c. Altere o valor do parâmetro Willingness de 5 para 0.
    d. Verifique se o protocolo do valor RedirectingURL está listado como https.
    e. Altere o valor RedirectingURL <cgi directory> de CAisd para CAisdsec.
    f. Salve as mudanças.
2. No caso de mecanismos não seguros que lidam com as outras atividades, edite o arquivo <*Host_Name*>-web[#].cfg para os mecanismos da web não seguros que você quer que lidem com as atividades sem logon. Verifique se o valor do parâmetro CAisd é /CAisd.
    a. Altere o valor do parâmetro UseDirector de Yes para BeforeLogin.
    b. Mantenha o valor de Willingness em 5 ou defina-o com qualquer valor de número inteiro de 1 a 10, dependendo da carga desejada.

c. Verifique se o protocolo do valor RedirectingURL está listado como http.

d. Verifique se o valor RedirectingURL <cgi directory> é CAisd.

e. Salve as mudanças.

Os valores de parâmetro do web director são verificados.

Os mecanismos da Web de logon seguro devem residir no diretório físico mapeado ao diretório virtual com proteção SSL (nesse caso, 'CAisdsec').

Você pode verificar o ambiente de logon SSL quanto a mecanismos da web, como segue:

- Os mecanismos da web de logon seguro devem residir no diretório físico mapeado para o diretório virtual com proteção SSL (nesse caso, CAisdsec).

  No caso de mecanismos da web com logon seguro, crie instâncias de pdmweb.exe no diretório $NX_ROOT/bopcfg/www/ wwwrootsec usando o nome pdmweb[#].exe. O nome do executável deve corresponder ao valor de CGI I/F de cada mecanismo da web com logon seguro definido em pdm_edit.pl.

  Exemplo: se pdm_edit.pl receber a atribuição do valor de CGI I/F pdmweb2 do mecanismo da web de logon seguro, crie uma cópia física de pdmweb.exe e renomeie-a como pdmweb2.exe.

- Os web directors e mecanismos da web não-seguros devem residir no diretório físico mapeado para o diretório virtual não-SSL CAisd.

  No caso de web directors e mecanismos da web não-seguros, crie instâncias de pdmweb.exe no diretório $NX_ROOT/bopcfg/www/wwwroot. Deve haver uma cópia de pdmweb.exe para cada mecanismo da web e web director não-seguro definido em pdm_edit.pl. Renomeie as cópias de modo que os novos nomes dos executáveis correspondam aos valores de CGI I/F definidos para os mecanismos da web e web directors em pdm_edit.pl.

  Exemplo: se pdm_edit.pl receber a atribuição do valor de CGI I/F pdmweb3 do mecanismo da web de logon não-seguro, e do valor pdmweb_d1 do web director, crie duas cópias de dmweb.exe. Renomeie a primeira cópia como pdmweb3.exe e depois renomeie a segunda como pdmweb_d1.exe.

Servidores secundários e recursos da web

Todos os sistemas têm um servidor primário. O servidor primário hospeda os serviços básicos de sistema, como o hub de comunicações e o banco de dados. Muitos usuários empresariais distribuem o sistema para outros servidores, denominados servidores secundários. Nesse tipo de configuração, você pode adicionar recursos da web aos servidores secundários.

Como preparar recursos da web

As tarefas de pré-requisito para adicionar recursos de web a servidores secundários (e se você estiver implementando um ambiente de logon SSL) são as seguintes:

1. Verifique se os servidores primários e secundários estão instalados e configurados.
2. Verifique se o servidor web com SSL que hospeda o mecanismo da web de logon seguro importou um certificado SSL.
3. No servidor web que hospeda o mecanismo da web de logon seguro, crie uma cópia física (incluindo subdiretórios) do diretório $NX_ROOT/bopcfg/www/wwwroot e o nomeie como $NX_ROOT/bopcfg/www/wwwrootsec.
4. Defina um novo diretório virtual chamado CAisdsec para o servidor web.
5. Aponte o diretório virtual para o diretório físico $NX_ROOT/bopcfg/www/wwwrootsec.
6. Verifique se as permissões do diretório virtual para CAisdsec correspondem às permissões do diretório virtual CAisd para execução de scripts.
7. Ative o SSL para o diretório virtual CAisdsec.

   Observação: o nome CAisdsec é definido pelo usuário e você pode renomeá-lo.

Como criar um sistema com servidores secundários

Para criar um sistema com servidores secundários, faça o seguinte:

1. Usando o pdm_edit.pl, adicione ou edite as entradas do web director. Um WebDirector pode distribuir a carga entre vários mecanismos da Web. Adicione mecanismos da web e web directors a outros servidores. Ao especificar um servidor secundário, use o mesmo nome com o qual o servidor secundário foi configurado. Esse nome é o valor de NX_LOCAL_HOST no arquivo NX.env no servidor secundário.

   Observação: a atribuição automática de CGI I/F do web director atribui nomes a partir do arquivo pdm_edit.pl: o nome pdmweb_d1.exe é atribuído automaticamente ao primeiro web director no servidor primário. O segundo web director no servidor primário será nomeado como pdmweb_d2.exe. O terceiro será nomeado pdmweb_d3.exe, e assim por diante. Um servidor secundário também pode ter web directors com os valores de CGI I/F pdmweb_d1.exe, pdmweb_d2.exe e pdmweb_d3.exe. Não há conflito de nome porque os nomes de web directors são exclusivos para o computador local em que os web directors estão sendo executados.

2. Cada mecanismo da Web deve fazer referência a um gerenciador de objeto. Sempre haverá um gerenciador de objetos denominado domsrvr. Você pode adicionar mais gerenciadores de objetos ao servidor secundário e atribuir a eles mecanismos da web como segue:

   - Número de mecanismos da web a adicionar — Durante a implementação de qualquer esquema de equilíbrio de carga de mecanismo da web, Logon SSL, ou ambos, atribua ao menos dois mecanismos da web ao mesmo web director.

   - Ambiente de logon SSL — Quando você definir o mecanismo da web de logon seguro em pdm_edit.pl, este mecanismo da web deve estar sob o controle de um web director. Defina o valor do parâmetro de protocolo do mecanismo da web de logon seguro como https. Esta configuração assegura que o web director criará o valor de URL de redirecionamento correto para o cliente web.

3. Salve as mudanças, saia do script pdm_edit.pl e especifique qual arquivo usar para um modelo do web.cfg quando solicitado.

   Observação: os web directors não usam um arquivo <*Host_Name*>-web[#].cfg. No entanto, mecanismos da web exigem um arquivo <*Host_Name*>-web[#].cfg exclusivo. Os arquivos web.cfg de exemplo são automaticamente gerados usando o script pdm_edit.pl ao salvar e sair do script. É solicitado que você especifique um arquivo web.cfg a ser usado como modelo na criação dos arquivos de configuração da web. Você pode importar as personalizações no arquivo web.cfg original para os novos arquivos de configuração da web especificando o web.cfg original como o arquivo de modelo desejado.

4. No servidor primário, salve as seguintes cópias de backup. Elas serão úteis se você quiser restaurar o ambiente original:

   ```
   $NX_ROOT/pdmconf/pdm_startup.tpl
   $NX_ROOT/pdmconf/pdm_startup
   $NX_ROOT/bopcfg/www/*web*.cfg
   $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
   ```

5. No servidor secundário, salve cópias de backup de qualquer arquivo $NX_ROOT/bopcfg/www/web.cfg ou <*secondary_name*>-web[#].cfg existente.

   $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*

6. No servidor primário, mova $NX_ROOT/samples/pdmconf/pdm_startup.rmt para $NX_ROOT/pdmconf e renomeie-o como pdm_startup.tpl.

7. Para cada mecanismo da web atribuído a um web director, verifique se o mecanismo da web <*Host_Name*>-web[#].cfg está definido corretamente, examinando o arquivo em um editor de texto. Se necessário, modifique os valores de parâmetro do web director para especificar a função do mecanismo da web que você quer.

8. No servidor primário; mova todos os arquivos de $NX_ROOT/samples/pdmconf/primary-web[#].cfg para o diretório $NX_ROOT/bopcfg/www.

9. Mova todos os arquivos $NX_ROOT/samples/pdmconf/'secondary_server_name-web[#].cfg' do servidor primário para o diretório $NX_ROOT/bopcfg/www do servidor secundário.

10. (Servidores servlet, como o Tomcat) Especifique um web.xml.tpl em cada diretório $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF. Quando você configura esse servidor, o processo de configuração cria um arquivo web.xml. O utilitário pdm_edit.pl criou arquivos web.xml.tpl de amostra. Cada arquivo é nomeado como <hostname>-web.xml.tpl. Você pode usar esses arquivos como exemplos: copie e renomeie-os como web.xml.tpl para cada um de seus servidores.

11. (Servidores HTTP, como o IIS ou Apache) Em cada servidor do CA SDM (primário, secundário, ou ambos) que você queira hospedar um mecanismo da web ou web director, crie cópias de pdmweb.exe no diretório $NX_ROOT/bopcfg/www/wwwroot. Um pdmweb[#].exe para cada mecanismo da web e um pdmweb_d[#].exe para cada web director definido no pdm_edit.pl para execução naquele servidor. Verifique se pdmweb[#].exe e pdmweb_d[#].exe estão nomeados com os valores de CGI I/F das definições do script pdm_edit.pl (por exemplo, pdmweb1.exe, pdmweb2.exe, pdmweb_d1.exe, etc.).

12. Se você estiver usando o IIS e quiser adicionar extensões de servidor para cada interface CGI, copie o arquivo primary-site.dat para o diretório $NX_ROOT/bopcfg/www como site.dat. Quando o sistema é reconfigurado, essas localidades são adicionadas ao IIS.

13. Reconfigure o servidor primário sem reinicializar o banco de dados e inicie os serviços.

14. Reconfigure os servidores secundários.

15. Para uma integração do Gerenciamento de conhecimento com CA SDM, se o SSL tiver sido imposto para CA SDM, o valor de protocolo do URL do CA SDM deve ser alterado.

    a. A partir do Gerenciamento de conhecimento, Gerenciador de configurações, Integração geral, altere o valor de protocolo do URL do CA SDM de http para https.

    b. Salve e saia.

16. Abra um navegador da web na página de logon do CA SDM e verifique se um usuário pode efetuar logon e se logon ou redirecionamento está adotando o comportamento esperado.

Configuração do servidor

pdm_edit.pl permite que você adicione funcionalidade e aumente o desempenho do sistema da empresa. Você pode configurar os serviços do CA SDM. O CA SDM tem daemons básicos no servidor primário. Você pode adicionar mais daemons ao servidor primário e, em seguida, expandir seu sistema por vários servidores, adicionando servidores secundários, o que aumenta o volume, o desempenho e a segurança.

Se você usar pdm_edit.pl para modificar a configuração do daemon, as personalizações disponíveis que usam pdm_configure serão desativadas. Por exemplo, após alterar o arquivo pdm_startup.tpl com o pdm_edit.pl, você não poderá ativar um web director ou conversor de evento usando a interface gráfica de usuário do pdm_configure. Você pode personalizar esses recursos usando o utilitário pdm_edit.pl.

O menu superior de pdm_edit.pl aparecerá depois que você executar pdm_edit.pl e inserir perguntas específicas do sistema operacional. Esse menu lista os recursos desse utilitário. Digitar um número desse menu o levará a submenus do recurso selecionado. A partir dos submenus, você poderá retornar ao menu superior. No final da sessão, selecione "Sair sem salvar" ou "Salvar e sair". Isso criará um arquivo pdm_startup.dat, que é um resumo de todas as suas seleções. Guarde esse arquivo para que você possa continuar mais tarde. O utilitário cria um arquivo pdm_startup.rmt e serve como uma substituição para o arquivo $NX_ROOT/pdmconf/pdm_startup.tpl em seu servidor primário. Após instalar o arquivo pdm_startup.rmt como pdm_startup.tpl no servidor primário, reconfigure sem reinicializar seu banco de dados para ativar as mudanças.

Observação: os nomes de host de todos os servidores secundários fazem distinção entre letras maiúsculas e minúsculas e representam o valor NX_LOCAL_HOST no arquivo NX.env no servidor secundário

Execute o pdm_edit.pl em um servidor UNIX

Você pode executar o pdm_edit.pl em um servidor UNIX. Você deve ter uma instalação do servidor primário e, opcionalmente, um servidor secundário instalado e configurado para todos os documentos do CA SDM relevantes.

Observação: execute pdm_edit.pl apenas no servidor primário. Para obter mais informações sobre servidores secundários executando a interface da web, consulta o Guia de Implementação.

Para executar o pdm_edit.pl em um servidor UNIX

1. Na linha de comando do servidor primário, altere para o seguinte local:

   ```
   Diretório $NX_ROOT/samples/pdmconf.
   ```

2. Insira o seguinte comando:

   ```
   '$NX_ROOT/bin/pdm_perl pdm_edit.pl'
   ```

   O executável pdm_perl do CA SDM executa o script pdm_edit.pl. Várias opções de menu e prompts permitem adicionar, modificar ou excluir os gerenciadores de objetos, web directors e mecanismos da web e, em seguida, salvar as mudanças ou adições em arquivos pdm_startup.dat e pdm_startup.rmt no servidor primário.

Execute o pdm_edit.pl em um servidor Windows

Você pode executar o pdm_edit.pl em um servidor Windows. Você deve ter uma instalação do servidor primário e, opcionalmente, um servidor secundário instalado e configurado para todos os documentos do CA SDM relevantes.

Observação: execute pdm_edit.pl apenas no servidor primário. Para obter mais informações sobre servidores secundários executando a interface web, consulta o Guia de Implementaçã*o*.

Para executar o pdm_edit.pl em um servidor Windows

1. Abra uma janela de prompt de comando e passe ao seguinte diretório:

   ```
   %diretório_instalação\samples\pdmconf.
   ```

2. Insira o seguinte comando:

   ```
   %installation-directory\samples\pdmconf\pdm_perl pdm_edit.pl
   ```

   O executável pdm_ erl executa o script pdm_edit.pl. Várias opções de menu e prompts com base em texto são exibidos para permitir ao usuário adicionar, modificar ou excluir os gerenciadores de objetos, web directors e mecanismos da web e, em seguida, salvar as mudanças ou adições em arquivos pdm_startup.dat e pdm_startup.rmt no servidor primário.

Gerenciadores de objeto

Os gerenciadores de objetos administram todos os objetos do CA SDM. Há sempre um Gerenciador de objetos no servidor primário. Cada gerenciador de objetos tem um nome, que é similar ao nome que ele usa para se comunicar com outros objetos. O gerenciador de objetos padrão no servidor primário sempre é denominado domsrvr. Sistemas empresariais com servidores multiprocessador ou servidores secundários podem adicionar mais gerenciadores de objetos ao servidor primário e servidores secundários. Você pode navegar, adicionar, editar e excluir gerenciadores de objetos.

Um host é atribuído a cada gerenciador de objetos. Os gerenciadores de objetos atribuídos ao servidor primário sempre utilizam primary como nome do host.

Você pode agrupar gerenciadores de objetos, de modo que os grupos sejam atribuídos para fornecer serviço a grupos específicos de mecanismos da web e clientes Java. Geralmente, não é necessário definir um *grupo*, pois o recurso de equilíbrio de carga do sistema distribui a carga por todos os gerenciadores de objetos. Os usuários que precisam desse recurso em geral têm mecanismos da web separados geograficamente do servidor primário e gostariam de posicionar um gerenciador de objetos perto do mecanismo da web. Os usuários agrupam os gerenciadores de objetos atribuídos aos mecanismos da web locais e, em seguida, atribuem os mecanismos da web a esse grupo de gerenciadores de objetos.

A Máscara de aceitação é um recurso avançado que indica ao gerenciador de objetos de quais clientes ele aceita conexões. Normalmente, um mecanismo da web tenta se conectar a um gerenciador de objetos com um nome como web:seattle:1, web:seattle:2 ou web:texas:1. O administrador pode especificar uma máscara Aceitar, como web:seattle.*, para aceitar todas as conexões de seattle e rejeitar as outras. O administrador também pode especificar uma máscara como web:.* para aceitar conexões de mecanismos da web e rejeitar conexões de clientes.

O recurso do valor de Exibição também pode ser útil. A maioria dos usuários permite que o sistema defina o nome do host como padrão. Esse valor aparece no cliente para indicar a qual gerenciador de objetos ele está conectado.

Entrar e sair do Gerenciador de objetos

A instalação do CA SDM fornece por padrão um gerenciador de objetos no servidor primário. O gerenciador de objetos padrão, comm. nome comm. = 'domsrvr', não é exibido na lista Gerenciadores de objeto; no entanto, saiba que ele está presente e é iniciado quando o Gerenciador de daemon do CA SDM é iniciado.

Para entrar e sair do Gerenciador de objetos

1. No menu superior de pdm_edit.pl, selecione 1 e pressione Enter.

   O submenu Gerenciador de objetos aparece.

2. Pressione Enter.

   Saia do submenu Gerenciador de objetos, e o menu de nível superior de pdm_edit.pl aparecerá.

Adicionar gerenciadores de objetos

Você pode adicionar gerenciadores de objetos ao submenu Gerenciador de objetos.

Para adicionar gerenciadores de objetos

1. No submenu Gerenciador de objetos, selecione a, depois pressione Enter.

   Um prompt solicita o nome do host.

2. Pressione Enter para selecionar o valor padrão de servidor primário ou digite um valor para o nome do host do servidor secundário.

   Observação: os nomes do host de todos os servidores secundários fazem distinção entre letras maiúsculas e minúsculas e são o valor NX_LOCAL_HOST no arquivo NX.env no servidor secundário.

3. Pressione Enter.

   Um prompt solicita o grupo.

4. Pressione Enter para aceitar o valor padrão 'Nenhum' ou digite um nome de grupo e pressione Enter.

   Um prompt solicita a máscara de aceitação.

   Observação: uma máscara de aceitação é um filtro que restringe a comunicação do gerenciador de objetos a somente aqueles processos com um nome que corresponda à máscara de aceitação.

5. Pressione Enter para aceitar o valor padrão 'Não aceitar' ou digite a seqüência de caracteres da máscara de aceitação que você quer usar.

   Um prompt solicita o valor Nome de exibição do Gerenciador de filas.

6. Pressione Enter para aceitar o padrão ou digite um valor para Nome de exibição e pressione Enter.

   O submenu Gerenciador de objetos aparece e o gerenciador de objetos adicionado mais recentemente é listado.

Editar um gerenciador de objetos

Você pode editar gerenciadores de objetos.

Para editar um gerenciador de objetos

1. No submenu Gerenciador de objetos, selecione e, depois pressione Enter.

   Um prompt solicita que você informe a chave.

   Observação: o valor dessa chave é mostrado na lista de gerenciadores de objetos e é criado automaticamente sempre que um gerenciador de objetos é adicionado. A chave está no formato nome do host: # # é um número inteiro em requisição seqüencial, com o número máximo igual ao número total de gerenciadores de objetos no host especificado. Por exemplo, se houver dois gerenciadores de objetos no servidor primário e dois gerenciadores de objetos em um servidor secundário (host name=‘godzilla’), as chaves serão: ‘primary:'1’, ‘primary:2’, ‘godzilla:1’ e ‘godzilla:2’.

2. Insira a chave (godzilla:1) e pressione Enter.

   Um prompt solicita o grupo.

3. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o inserindo um valor de grupo e pressione Enter.

   Um prompt solicita a máscara de aceitação.

4. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o inserindo um valor de máscara de aceitação e pressione Enter.

   Um prompt solicita a exibição.

5. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o inserindo um valor de exibição e pressione Enter.

   O submenu Gerenciador de objetos aparece, e o gerenciador de objetos é editado.

Excluir um gerenciador de objetos

Você pode excluir um gerenciador de objetos.

Para excluir um gerenciador de objetos

1. No submenu Gerenciador de objetos, selecione d, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Observação: se você inserir a chave errada (o que exclui a entrada domsrvr errada), saia do script pdm_edit.pl *sem* salvar as mudanças.

   O gerenciador de objetos é excluído, e o submenu Gerenciador de objetos aparece.

Como especificar web directors

Os Webdirectors são opcionais e são usados quando os sistemas exigem dois ou mais mecanismos da Web. Os web directors servem para equilibrar a carga entre os mecanismos da web. Pode haver zero ou mais web directors. Cada web director equilibra a carga entre dois ou mais mecanismos da web.

Para especificar um web director, execute as seguintes etapas:

1. Indique o nome do host.

   Se o web director estiver no servidor primário, digite “primary”; do contrário, digite o nome do servidor secundário. O nome do servidor secundário é a entrada NX_LOCAL-HOST no arquivo NX.env no servidor secundário.

   Observação: use as letras maiúsculas e minúsculas exatamente como fornecidas.

2. (Opcional) Especifique a interface CGI.

   Na maioria de casos, o valor padrão é apropriado. Se você estiver usando um servidor HTTP, como IIS ou Apache, esse valor é arquivo do CGI executado em resposta a uma solicitação do CGI (o nome do executável do CGI). Crie cópias de pdmweb.exe no diretório $NX_ROOT/bopcfg/www/wwwroot usando esse nome. Se você estiver usando um servidor servlet, como o Tomcat, um arquivo de amostra web.xml.tpl será criado. Use esse arquivo para substituir o arquivo web.xml.tpl no diretório $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF do servidor específico. Cada arquivo de amostra web.xml.tpl é criado no diretório atual e nomeado <nome_host>-Web.xml.tpl.

Entrar e sair do web director

Definir um web director adiciona apenas as informações do web director. Esse web director é usado pelo CA SDM apenas quando um ou mais mecanismos da web são atribuídos a ele. Você pode entrar e sair do web director.

Para entrar e sair do web director

1. No menu superior de pdm_edit.pl, selecione d, depois pressione Enter.

   O submenu Web Director aparece.

2. Pressione Enter.

   Saia do submenu Web Director e o menu superior de pdm_edit.pl aparece.

Adicionar web directors

Você pode adicionar web directors. Cada web director definido em pdm_edit.pl deve ter um valor exclusivo de CGI I/F. O nome de CGI I/F é automaticamente gerado; no entanto, o nome CGI I/F sugerido pode ser manualmente substituído para refletir qualquer esquema de nomenclatura CGI que você quiser.

Considere o seguinte antes de adicionar web directors:

- Se você estiver usando um servidor HTTP, como IIS ou Apache, deverá ter um pdmweb_d[#].exe nomeado corretamente no diretório $NX_ROOT/bopcfg/www/wwwroot.
- Se você estiver usando um servidor servlet, como o Tomcat, um arquivo de exemplo web.xml.tpl é criado. Esse arquivo é nomeado <*hostname*>-web.xml.tpl e está localizado no diretório de trabalho. Use esse arquivo para substituir o arquivo $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml.tpl no servidor apropriado.

Para adicionar web directors

1. No submenu Web Director, selecione a, depois pressione Enter.

   Um prompt solicita o nome do host.

2. Pressione Enter para selecionar o valor padrão de Primário ou digite um valor para o nome do host do servidor secundário.
3. Pressione Enter.

   Um prompt solicita um nome para a interface CGI.

4. Pressione Enter para aceitar o valor exibido ou digite manualmente o valor desejado e pressione Enter.

   O submenu Web Director aparece, e o web director adicionado mais recentemente é listado.

Editar um web director

Você pode editar um web director.

Para editar um web director

1. No submenu Web Director, selecione e, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Um prompt solicita um valor de CGI I/F.

3. Pressione Enter para aceitar o valor exibido ou modifique-o, inserindo o valor de CGI I/F desejado e, em seguida, pressione Enter.

   O submenu Web Director aparece, e o web director é alterado.

Excluir um web director

Você pode excluir uma entrada do web director.

Para excluir uma entrada do web director

1. No submenu Web Director, selecione d, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Observação: se você inserir a chave errada (que exclui a entrada errada do web director), saia do script pdm_edit.pl *sem* salvar as mudanças.

   O submenu Web Director aparece, e a entrada do web director é excluída.

Alterar o valor de CGI I/F para um web director

Você pode alterar o valor de CGI I/F para um web director.

Para alterar o valor CGI/IF

1. No submenu web director, selecione c, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Um prompt solicita um valor de CGI I/F.

3. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o, inserindo o valor de CGI I/F desejado e, em seguida, pressione Enter.

   O submenu Web Director aparece, e o valor de CGI I/F para o web director é alterado.

Mecanismos da Web

Os mecanismos da web ajudam a preparar páginas da web para o cliente web. Os sistemas podem ter um ou mais mecanismos da web. Zero ou mais mecanismos da web podem existir em cada servidor. Você pode navegar, adicionar, editar e excluir mecanismos da web. Cada mecanismo da web se conecta a um gerenciador de objetos para processar todas as solicitações a objetos do CA SDM. O padrão é conectar-se ao gerenciador de objetos padrão, mas se você tiver mais de um gerenciador de objetos, poderá definir esse valor como ANY.

Ao definir um mecanismo da web, especifique o nome do host. Insira **primary** para todos os mecanismos da web que iniciam no servidor primário; ou insira o nome do host do servidor secundário. O nome do host faz distinção entre letras maiúsculas e minúsculas e deve corresponder à entrada NX_LOCAL_HOST no NX.env do servidor secundário.

Cada mecanismo da Web pode ser executado e acessado diretamente. Em acesso direto, cada navegador da web entra na interface específica de CGI para o mecanismo da web, e os usuários determinam a carga do sistema (o equilíbrio de carga não é automatizado). Todos os clientes podem se conectar a um mecanismo da web e sobrecarregá-lo, enquanto os outros mecanismos da web não são usados. Uma melhor abordagem é atribuir dois ou mais mecanismos da web a um único web director. Todas as solicitações enviadas a um desses mecanismos da web são direcionadas ao web director para equilíbrio de carga e, em seguida, redirecionadas para o mecanismo da web mais disponível no grupo.

Outras configurações podem incluir web directors. Uma delas direciona todos os logons a um único mecanismo da web SSL seguro, que controla todos os logons. Depois de efetuar logon, o cliente é direcionado para outro mecanismo da Web disponível para processamento posterior.

Interface CGI

Cada mecanismo da web tem e usa uma interface CGI como segue:

- Quando é usado um servidor HTTP, como IIS ou Apache, a interface é um executável armazenado no diretório $NX_ROOT/bopcfg/www/wwwroot. O nome da interface CGI é o nome do executável. Os navegadores inserem a interface CGI na linha de endereço e a solicitação é direcionada ao mecanismo da Web apropriado.
- Ao usar um servidor de servlet como Tomcat, a interface CGI é simulada por um servlet. Cada servidor de servlet tem um arquivo web.xml.tpl que descreve todas as interfaces CGI. O utilitário pdm_edit.pl cria arquivos web.xml.tpl de exemplo denominados <*hostname*>-web.xml.tpl. Use os arquivos para substituir o arquivo web.xml.tpl no servidor apropriado e reconfigure o servidor.
- Ao usar um web director, geralmente é útil definir uma interface CGI de um mecanismo da web com um nome CGI conhecido. Todas as solicitações irão para esse mecanismo da web e serão redirecionadas para um mecanismo da web mais disponível. Esta instalação permite aos usuários lembrar somente um único nome de interface CGI. Além disso, todas as solicitações são equilibradas através de todos os mecanismos da web disponíveis.

Entrar e sair do mecanismo da web

Por padrão, o CA SDM instala e configura um mecanismo da web no servidor primário (chave= primária:1; gerenciador de objetos= domsrvr; CGI I/F= 'pdmcgi', protocolo= não especificado).

Para entrar e sair do mecanismo da web

1. No menu superior de pdm_edit.pl, selecione w, depois pressione Enter.

   O submenu do mecanismo da web aparece.

2. Pressione Enter.

   Saia do submenu do mecanismo da web, e o menu de nível superior de pdm_edit.pl aparece.

Considerações para adicionar mecanismos da web

Considere as seguintes informações ao adicionar mecanismos da web:

- **Direcionar clientes a mecanismos da web** — Você pode especificar como clientes da web são direcionados a mecanismos da web. Por exemplo, considere dois web directors que estão sendo usados, miko:1 e godzilla:1. miko:1 tem quatro mecanismos da web atribuídos a ele, godzilla:1, godzilla:2, godzilla:3 e primary:3. Qualquer cliente web pode solicitar https:godzilla:8080/Caisd/ComputerAssociates.exe e ser redirecionado a qualquer um dos quatro mecanismos da web neste grupo. Se um cliente da web inserir http://localhost:8080/CAisd/pdmweb6.exe, o cliente sempre será direcionado a este mecanismo da web. Além disso, observe que alguns mecanismos da web são atribuídos ao gerenciador de objetos chamado domsrvr, e outros estão configurados para ser vinculados a QUALQUER gerenciador de objetos.
- **Usar valores CGI I/F** — Cada mecanismo da web definido em pdm_edit.pl deve ter um valor exclusivo de CGI I/F:
  - Se estiver usando um servidor HTTP, como IIS ou Apache, você deve ter um executável nomeado corretamente como pdmweb[#].exe no diretório $NX_ROOT/bopcfg/www/wwwroot.
  - Se você estiver usando um servidor servlet, como o Tomcat, um servlet substituirá a interface CGI. Esses servidores devem ter um arquivo web.xml.tpl no diretório $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF que descreve cada interface CGI. O utilitário pdm_edit.pl cria arquivos web.xml.tpl de exemplo denominados <*hostname*>-web.xml.tpl. Use esses arquivos para substituir o arquivo web.xml.tpl e reconfigure o servidor.

Adicionar mecanismos da Web

Você pode adicionar mecanismos da web.

Para adicionar mecanismos da web

1. No submenu do mecanismo da web, selecione a, depois pressione Enter.

   Um prompt solicita o nome do host.

2. Pressione Enter para selecionar o valor padrão de Primário ou digite um valor para o nome do host do servidor secundário.
3. Pressione Enter.

   Um prompt solicita o nome do gerenciador de objetos.

4. Pressione Enter para aceitar o valor padrão <primary domsrvr> ou digite manualmente uma combinação de alias e de nomes de comunicação de domsrvr, depois pressione Enter.

   Um prompt solicita a chave do web director.

5. Pressione Enter para selecionar o valor padrão Nulo (nenhum web director), ou digite um dos web directors listados pelo valor de chave, depois pressione Enter.

   Um prompt solicita um nome para a interface CGI.

6. Pressione Enter para aceitar o valor exibido ou digite manualmente um valor e pressione Enter.

   Se um web director não tiver sido especificado para este mecanismo da web, o submenu do mecanismo da web aparecerá. Se um valor do web director tiver sido especificado ou se ele já existia na definição do mecanismo da web, um prompt solicita que você especifique o protocolo a ser usado como prefixo para o valor do URL de redirecionamento do mecanismo da web.

7. Pressione Enter se você não quiser pré-anexar um prefixo de protocolo ao valor de redirecionamento de URL.

8. Digite **http** para anexar o prefixo de protocolo http ao valor de redirecionamento, a menos que SSL seja aplicado por esse mecanismo da Web. Por exemplo, digite **https** para anexar o prefixo de protocolo https ao valor de redirecionamento.

   Observação: se um web director tiver sido definido para esse mecanismo da web, o web director controla o redirecionamento para esse mecanismo da web, usando o valor do URL de redirecionamento. Se o protocolo SSL não for usado para esse mecanismo da web, especifique **http** ou nenhum. Se o protocolo SSL for imposto para esse mecanismo da web, especifique **https**. A falha ao especificar https para um mecanismo da web sob o SSL pode resultar em uma falha de redirecionamento do web director.

9. Pressione Enter.

   O submenu do mecanismo da web aparece, e o mecanismo da web adicionado mais recentemente é listado.

Editar um mecanismo da web

Você pode editar um mecanismo da web.

Para editar um mecanismo da Web

1. No submenu do mecanismo da web, selecione e, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Um prompt solicita que você insira o gerenciador de objetos.

3. Pressione Enter para aceitar o valor exibido como ele está ou modifique-o, inserindo o valor do gerenciador de objetos desejado e, em seguida, pressione Enter.

   Um prompt solicita um web director.

4. Pressione Enter para aceitar o valor exibido como ele está ou modifique-o, inserindo o valor do web director desejado e, em seguida, pressione Enter.

   Um prompt solicita um valor de CGI I/F.

5. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o, inserindo o valor de CGI I/F desejado e, em seguida, pressione Enter.

   Um prompt solicita o protocolo HTTP.

6. Pressione Enter para aceitar o valor exibido 'como está' ou modifique-o, inserindo o valor do protocolo HTTP desejado e, em seguida, pressione Enter.

   O submenu do mecanismo da web aparece.

Excluir um mecanismo da web

Você pode excluir um mecanismo da web.

Para excluir um mecanismo da Web

1. No submenu do mecanismo da web, selecione d, depois pressione Enter.

   Um prompt solicita que você informe a chave.

2. Insira a chave desejada e pressione Enter.

   Observação: se você inserir a chave errada (que exclui a entrada errada do mecanismo da web), saia do script pdm_edit.pl *sem* salvar as mudanças.

   O mecanismo da web é excluído e o submenu do mecanismo da web aparece.

Fazer mudanças usando pdm_edit.pl

É possível usar o utilitário pdm_edit.pl para adicionar e mover conversores, servidores, daemons e aliases no sistema do CA SDM.

Adicionar um conversor TNG

O utilitário pdm_edit.pl permite adicionar um único conversor de TNG a qualquer um dos servidores do seu sistema.

Observação: se o Gerenciador de daemon administrar o conversor de TNG, esse daemon será iniciado e interrompido com os outros daemons. Se o conversor de TNG for necessário para capturar eventos depois que os daemons do CA SDM forem encerrados, o conversor de TNG não poderá atender a este requisito. Portanto, inicie e pare o conversor de TNG como um serviço.

Para adicionar um conversor TNG

1. No menu superior de pdm_edit.pl, selecione T, depois pressione Enter.

   O submenu do conversor de TNG aparece.

2. No submenu do conversor de TNG, selecione A, depois pressione Enter.

   Um prompt solicita um nome de host.

3. Digite **primary** para o servidor primário ou o nome do host de um servidor secundário, depois pressione Enter.

   Um prompt solicita um endereço IP.

4. Insira **HOST_IP_REPLACE** se o conversor de TNG estiver no servidor primário; caso contrário, insira o IP do servidor secundário.

   O conversor de TNG é adicionado ao servidor.

Adicionar um conversor de UNIX

O utilitário pdm_edit.pl permite adicionar um único conversor de UNIX a qualquer um dos servidores do seu sistema.

Para adicionar um conversor UNIX

1. No menu superior de pdm_edit.pl, selecione N, depois pressione Enter.

   O submenu do conversor de UNIX aparece.

2. Selecione A, depois pressione Enter.

   Um prompt solicita um nome de host.

3. Digite **primary** para o servidor primário ou o nome do host de um servidor secundário, depois pressione Enter.

   Um prompt solicita um endereço IP.

4. Insira **HOST_IP_REPLACE** se o conversor de UNIX estiver no servidor primário; caso contrário, insira o IP do servidor secundário.

   O conversor de UNIX é adicionado ao servidor.

Mover validação do logon

O servidor de validação de logon usa o sistema operacional local para validar solicitações de usuário. O daemon de validação inicia no servidor primário por padrão, mas você pode movê-lo para um servidor secundário no qual todos os usuários tenham contas do sistema operacional, ou para um servidor com um tipo de sistema operacional diferente.

Para mover a validação do logon

1. No menu superior de pdm_edit.pl, selecione U, depois pressione Enter.

   O submenu do servidor de validação de usuário aparece.

2. Digite **E** para especificar o nome do host do servidor e pressione Enter.

3. Digite **primary** para o servidor primário ou o nome do host do servidor secundário e pressione Enter.

   A validação de logon é movida.

Mover um servidor LDAP

O servidor LDAP (Lightweight Directory Access Protocol) é instalado no servidor primário por padrão, mas pode ser movido para qualquer servidor secundário.

Para mover o servidor LDAP

1. No menu superior de pdm_edit.pl, selecione L, depois pressione Enter.

   O submenu do servidor LDAP aparece.

2. Digite **E** para especificar o nome do host do servidor, digite **primary** para o servidor primário ou o nome do host do servidor secundário.

   O servidor LDAP é movido.

Adicionar daemons de repositório

Um daemon de repositório existe no servidor primário por padrão, mas você pode adicionar outros.

Para adicionar daemons de repositório

1. No menu superior de pdm_edit.pl, selecione R, depois pressione Enter.

   O submenu do daemon de repositório aparece.

2. Digite **A** para especificar o nome do host do servidor.
3. Digite **primary** para o servidor primário ou o nome do host do servidor secundário.

   O daemon de repositório é adicionado ao servidor.

Criar um exemplo de alias

Alias são opcionais no CA SDM. Este exemplo mostra como se preparar para criar um alias e como criá-lo.

Exemplo: preparar-se para criar um alias

Antes de criar um alias, faça o seguinte:

1. Defina gerenciadores de objetos e adicione alguns deles a grupos. Os nomes dos gerenciadores de objetos são: domsrvr:group1:11, domsrvr, domsrvr:seattle:12, domsrvr;seattle:13, domsrvr:Tacoma:11.
2. Defina mecanismos da web e atribua gerenciadores de objetos aos mecanismos da web. Se você aceitar o padrão, o domsrvr é atribuído ao gerenciador de objetos.
3. Insira uma expressão comum que corresponda a um grupo de gerenciadores de objetos. Se o mecanismo da web se conectar a qualquer gerenciador de objetos, insira ANY. ANY é um alias padrão. Os mecanismos da web e clientes Java usam alias para especificar ANY ou um subconjunto dos gerenciadores de objetos em execução ao qual eles possam se conectar. Por exemplo, você quer que os clientes Java localizados em Washington se conectem a gerenciadores de objetos localizados em Seattle. Você os conecta a /domsrvr:seattle.*. Você também pode definir um alias chamado SEATTLE e atribuir a ele o valor /domsrvr:seattle.*.

Exemplo: criar um alias

Este exemplo considera que você definiu um gerenciador de objetos e o associou a um grupo chamado seattle. Se isso não tiver sido feito, o alias será criado, mas um aviso será exibido. Este aviso indica que o alias definido não corresponde a nenhum gerenciador de objetos existente.

1. No menu superior de pdm_edit.pl, selecione A, depois pressione Enter.

   O submenu Alias aparece.

2. Digite um nome para seu alias. Nesse exemplo, digite **SEATTLE**.

   Você será solicitado a digitar a expressão comum a ser associada a esse alias.

3. Digite **/domsrvr:seattle.***, que corresponderá a qualquer gerenciador de objetos com um nome que comece com domsrvr:seattle. Você pode usar esse alias ao configurar mecanismos da web e clientes Java.

4. Salve e saia do utilitário pdm_edit.pl.

   Um script de instalação de alias (chamado alias_install.bat ou alias_install.sh) é criado.

5. Execute o script de instalação de alias em seu servidor primário. Isso cria os alias e os transmite a todos os servidores secundários e clientes Java.

Mover daemons de conhecimento

Os daemons de conhecimento fornecem a base de conhecimento para o CA SDM. Eles são instalados no servidor primário por padrão, mas você pode usar o utilitário pdm_edit.pl para movê-los para servidores secundários.

Para mover daemons de conhecimento

1. No menu superior de pdm_edit.pl, selecione K, depois pressione Enter.

   O submenu Daemons de conhecimento aparece.

2. Digite **E** para alterar o host.

3. Digite **primary** para o servidor primário ou o nome do host do servidor secundário.

   Os daemons de conhecimento são movidos.

Considerações sobre a instalação de personalizações

Considere o seguinte ao instalar personalizações:

- pdm_edit.pl cria um arquivo pdm_startup.dat. Mantenha esse arquivo para que possa editar suas seleções atuais.
- pdm_edit.pl cria um arquivo pdm_startup.rmt. Esse arquivo é uma substituição para o arquivo pdm_startup.tpl localizado no servidor primário do diretório $NX_ROOT/pdmconf.
- Se você estiver usando um servidor servlet, como o Tomcat, um servlet substituirá a interface CGI. Esses servidores precisam de um arquivo web.xml.tpl. pdm_edit.pl cria um arquivo <*hostname*>-web.xml.tpl para cada servidor web. Use o arquivo apropriado para substituir o arquivo web.xml.tpl no diretório $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF em cada um dos servidores servlet.
- Se você estiver usando um servidor HTTP, como IIS ou Apache, crie executáveis da interface CGI no diretório NX_ROOT/bopcfg/www/wwwroot, copiando e renomeando o arquivo pdmweb.exe. Faça essa cópia e renomeie-a para todas as interfaces CGI de mecanismos web e web directors em todos os servidores que hospedam um cliente web.
- Cada mecanismo da web precisa de um arquivo web.cfg. pdm_edit.pl lista os arquivos web.cfg e os nomes a serem usados para salvá-los no servidor apropriado. Por exemplo, no servidor primário, existem seis destes arquivos. Nomeie um como web.cfg e o outro como primary-web2.cfg. pdm_edit.pl cria arquivos de exemplo web.cfg para cada mecanismo da web. Copie-os para o diretório $NX_ROOT/bopcfg/www do servidor apropriado.
- Se você estiver usando o IIS e for necessário adicionar extensões de servidor a cada interface CGI, pdm_edit.pl criará arquivos <*hostname*>-site.dat. Copie os arquivos para os servidores apropriados e renomeie-os como site.dat no diretório $NX_ROOT/bopcfg/www.
- Se você definiu aliases, execute o arquivo alias_install.sh ou alias_install.bat no servidor primário.
- Reconfigure todos os servidores secundários.
- Reconfigure o servidor primário sem reinicializar o banco de dados.

O submenu do mecanismo da Web é exibido novamente.

Você pode salvar mudanças em pdm_edit.pl e sair do utilitário.

Para salvar e sair do pdm_edit.pl

1. No menu superior de pdm_edit.pl, selecione x e pressione Enter.

   É solicitado que você selecione um arquivo de modelo. Esse arquivo de modelo serve como modelo para os arquivos web.cfg criados automaticamente para os mecanismos da web.

2. Selecione um dos valores exibidos. Por exemplo, selecione 2 para o arquivo web.cfg.tpl atualmente em uso no servidor primário. Essa seleção ajuda a assegurar que as personalizações instaladas no sistema sejam capturadas nos novos arquivos web.cfg.tpl de exemplo.

3. Pressione Enter.

   As mudanças são salvas e o prompt de comando aparece.

Iniciar o web director

Você pode iniciar o web director a partir da linha de comando ou configura o arquivo pdm_startup para iniciá-lo automaticamente.

Para iniciar o web director

1. Abra um prompt de comando.

2. Digite o seguinte comando:

   ```
   webdirector [–S nome_do_slump] [–c cgi]
   ```

3. Use as seguintes variáveis:

   slump_name

   Especifica o nome do slump do web director. O nome do slump identifica com exclusividade o processo do web director. Esse argumento é obrigatório apenas se você quiser iniciar mais de um web director. Caso contrário, recomendamos deixá-lo como seu valor padrão web:diretor.

   Cgi

   (Opcional) Especifica o nome do processo CGI usado para o web director. Se este argumento não for fornecido, a opção assumirá como padrão pdmweb_d1.exe.

O web director é iniciado e envia uma mensagem a todos os mecanismos da web em execução. Os mecanismos da web associados ao web director (ou seja, os configurados com UseDirector Yes, AfterLogin ou BeforeLogin, e WebDirectorSlumpName igual ao nome do slump do web director) respondem com suas definições de configuração. Quando um mecanismo da web configurado para usar o web director inicia, o mecanismo da web envia suas definições de configuração ao web director associado. Essa ação permite que o web director mantenha uma lista atualizada de todos os mecanismos da web ativos.

Como o web director lida com sessões de usuário

Você pode permitir aos usuários usar o URL de qualquer mecanismo da web ou o URL do web director para acessar o CA SDM.

Observação: se todos os mecanismos da web associados a um web director forem configurados com UseDirector Yes (ou seja, aqueles que não usam AfterLogin nem BeforeLogin), o web director funcionará apenas como um balanceador de carga.

O web director lida com sessões de usuário da seguinte maneira:

1. O URL do web director a seguir é publicado para os usuários:

   ```
   Windows e UNIX: http://hostname/CAisd/pdmweb_d1.exe
   ```

2. Ao receber uma solicitação, o web director faz o seguinte para o mecanismo da web:

   a. Determina se ele é mais capaz de lidar com a solicitação.

   b. Examina a contagem de sessão atual.

   c. Calcula a disposição atual usando a seguinte fórmula:

      ```
      aceitação atual = (aceitação configurada) / (contagem da sessão + 1)
      ```

3. O web director redireciona a solicitação ao mecanismo da web com a maior disposição atual.

4. O mecanismo da web selecionado controla a sessão inteira, do logon ao logout.

   Se um usuário no ambiente tentar acessar um mecanismo da web diretamente usando seu próprio URL, o mecanismo da web enviará uma mensagem ao web director pedindo uma referência. Se o web director responder com o URL de um mecanismo da web diferente, o mecanismo da web original redirecionará a sessão ao mecanismo da web recomendado.

Como configurar o web director em um ambiente SSL

Considere as seguintes informações se um ou mais mecanismos da web associados a um web director estiverem configurados com UseDirector AfterLogin, e os demais mecanismos da web estiverem configurados com UseDirector BeforeLogin:

- **UseDirector AfterLogin** — Ao receber uma solicitação, o web director determina o mecanismo da web mais adequado para controlar a solicitação, mas só seleciona a partir dos mecanismos da web com UseDirector AfterLogin. Para o logon, o web director considera os mecanismos da web com a disposição zero. Quando um mecanismo da web configurado com UseDirector AfterLogin recebe uma solicitação (por referência do mecanismo da web ou pelo usuário que está acessando diretamente seu URL), ele autentica o usuário usando qualquer método configurado no tipo de acesso do usuário. Após a autenticação do usuário, o mecanismo da web pede ao web director uma referência, e o web director novamente seleciona um mecanismo da web, dessa vez a partir de todos os mecanismos da web associados a ele e configurados com UseDirector BeforeLogin (com exceção daqueles com disposição zero). Quando o mecanismo da Web que está autenticando recebe a referência, ele transfere a sessão ao mecanismo da Web recomendado.
- **UseDirector BeforeLogin** — Se um usuário neste ambiente tentar acessar diretamente um mecanismo da web configurado com UseDirector BeforeLogin, o mecanismo da web enviará uma mensagem ao web director pedindo uma referência. O web director responde com uma referência a um mecanismo da web configurado com UseDirector AfterLogin, e o mecanismo da web original transfere a solicitação ao mecanismo da web recomendado.

Para configurar o web director em um ambiente SSL, recomendamos configurar um servidor HTTP para soquetes de segurança e associar um único mecanismo da web a esse servidor, como segue.

1. Leia e entenda como o web director lida com sessões (na página 426).
2. Configure o único mecanismo da web com UseDirector AfterLogin e WillingnessValue 0.

3. Configure um ou mais mecanismos da web adicionais para se conectar com um segundo servidor HTTP que use o protocolo HTTP padrão.
4. Configure esses mecanismos da web com UseDirector BeforeLogin e WillingnessValues apropriados à capacidade relativa de seus computadores host.

   O web director pode direcionar todos os logons para o servidor seguro (porque os servidores com disposição zero ainda estão qualificados para logon), mas indica o restante da sessão para um dos outros mecanismos da web.

Melhorar o desempenho com o armazenamento em cache no navegador

A interface da web do CA SDM usa muitos arquivos JavaScript, de imagem e folhas de estilo, que podem ser razoavelmente grandes e afetar o desempenho.

Para melhorar desempenho da interface da web, configure seu servidor HTTP de modo que o navegador armazene em cache esses arquivos, fazendo com que eles sejam carregados apenas uma vez por dia.

O desempenho da interface da web melhora.

Observação: a instalação padrão configura o armazenamento em cache automaticamente para o Apache e o IIS, mas você pode configurá-lo manualmente.

Configure o Microsoft Internet Information Server

É possível configurar o Microsoft Internet Information Server (IIS) para notificar o navegador de que arquivos carregados a partir do diretório do CA SDM expiram um dia após o carregamento. Isso significa que o navegador consulta o servidor sobre esses arquivos somente uma vez por dia, independentemente de quantas vezes eles são usados.

Para configurar o Microsoft Internet Information Server:

1. Inicie o aplicativo Internet Services Manager (para Windows 2000 e XP, selecionar Programas, Ferramentas administrativas, Internet Services Manager).
2. Navegue até a pasta de arquivos do CA SDM, que normalmente é CAisd.
   a. Clique no sinal de mais ao lado do servidor executando a interface da Web do CA SDM.
   b. Clique no sinal de mais ao lado de Site padrão.
   c. Role para baixo até CAisd.
3. Clique com o botão direito do mouse na pasta CAisd e selecione Propriedades.

   A página Propriedades aparece.
4. Clique na guia Cabeçalhos HTTP.
5. Marque a caixa de seleção Enable Content Expiration.
6. Selecione o botão de opção Expirar após, digite 1 no campo de texto e selecione um dia na lista suspensa.
7. Clique em OK.

   As propriedades estão salvas e as mudanças entram em vigor imediatamente.

Configurar Apache

É possível configurar o Apache para notificar o navegador de que arquivos carregados a partir do diretório do CA SDM expiram um dia após o carregamento. Essa configuração significa que o navegador consulta o servidor sobre estes arquivos somente uma vez por dia, independentemente de quantas vezes eles são usados.

Configure o Apache, atualizando um arquivo de configuração de texto. A instalação padrão modifica seu arquivo de configuração ativo no diretório apache conf (normalmente httpd.conf) para conter a instrução:

`Inclua` *`diretório de instalação`*`/bopcfg/www/CAisd_apache.conf`

diretório de instalação deve ser substituído por um caminho completo. No Windows, geralmente o caminho é c:\Arquivos de programas\CA\CA SDM. No UNIX, substitua *diretório de instalação* pelo valor de $NX_ROOT.

O arquivo CAisd_apache.conf, que é referenciado no comando Include, contém texto a seguir. Novamente, *diretório de instalação* é substituído pelo caminho completo como apareceu na instrução Include.

```
<IfModule mod_alias.c>
        Alias /CAisd diretório de instalação/bopcfg/www/wwwroot/
        <IfModule mod_expires.c>
                <Directory diretório de instalação/bopcfg/www/wwwroot>
                ExpiresActive   On
                ExpiresDefault  "access plus 1 day"
                </Directory>
        </IfModule>
</IfModule>
```

Para configurar o Apache manualmente o armazenamento em cache do navegador dos arquivos do CA SDM, inclua instruções semelhantes às do CAisd_apache.conf em seu arquivo de configuração do Apache. Você pode adicioná-los diretamente no arquivo ou adicionar uma instrução Include fazendo menção a um arquivo separado, como a instalação padrão.

As mudanças nos arquivos de configuração do Apache entram em vigor depois da reciclagem do Apache.

Limpar o cache

Se você alterar um arquivo JavaScript, de imagem, folha de estilos, HTML ou de ajuda carregado pelo próprio servidor HTTP, você deve instruir os usuários a limpar o cache do navegador.

Observação: para mudanças a arquivos HTMPL entrarem em vigor, é necessário reciclar o mecanismo da web ou usar o utilitário pdm_webcache. Em um ambiente de desenvolvimento, você pode evitar essa tarefa especificando a propriedade do arquivo de configuração SuppressHtmplCache.

Para limpar o cache do navegador para o Internet Explorer

1. Selecione Ferramentas, Opções da Internet.

   É exibida a caixa de diálogo Opções da Internet.

2. Clique em Excluir arquivos.

   Uma janela de confirmação é exibida.

3. Clique em OK.

   O cache do navegador é limpo.

Para limpar o cache do navegador para o Firefox

1. Selecione Ferramentas, Limpar área privada.
2. Clique no botão Limpar dados particulares agora.

   O cache do navegador é limpo.

Registrar o comportamento de bloqueio na interface da Web

Quando um usuário edita um registro de banco de dados usando a interface da Web, o usuário tem o registro bloqueado exclusivamente por dois minutos, que é o tempo padrão. É possível modificar o tempo padrão usando a propriedade ExclLockSeconds no arquivo web.cfg.

As seguintes condições afetam se um registro de banco de dados é atualizado pelas modificações de um usuário:

- Se um usuário *puder* editar e enviar as modificações dentro do tempo alocado, elas são incluídas no banco de dados.

  Durante o tempo em que o registro de banco de dados está bloqueado, outros usuários (Web e não-Web) podem visualizar o registro, mas não podem editá-lo. Se outro usuário tentar editar o registro enquanto ele estiver bloqueado, será exibida uma mensagem de erro.

- Se um usuário *não puder* editar e enviar as modificações dentro do tempo alocado, o bloqueio de registro é automaticamente removido e outros usuários podem editar o registro.

  Quando o usuário finalmente envia as atualizações, os carimbos de data e hora são verificados para garantir que mais ninguém alterou o registro e o seguinte ocorre:

  - Se o registro não tiver sido alterado desde a eliminação do bloqueio exclusivo, as atualizações do usuário serão salvas no banco de dados.
  - Se outro usuário editou o registro depois da expiração do bloqueio, o usuário recebe uma resposta de erro da tentativa de salvar e as mudanças não serão salvas. O usuário deve reiniciar o processo de edição e inserir novamente as modificações.

Mais informações:

Modificação de arquivo de configuração (na página 432)

Imprimir páginas da Web do CA SDM

O CA SDM usa gráficos de plano de fundo para formatar os botões e as guias do bloco de notas. A configuração padrão para muitos navegadores é *não* imprimir essas imagens de plano de fundo. Portanto, se você selecionar Arquivo, Imprimir em qualquer menu do navegador ou do CA SDM, a página impressa mostrará apenas os cantos dos botões ou das guias.

Para imprimir páginas da Web do CA SDM no Internet Explorer

1. Selecione Ferramentas, Opções da Internet.

   A caixa de diálogo Opções da Internet aparece.

2. Selecione a guia Avançado.
3. Role para baixo até o cabeçalho Impressão e marque a selecione a opção Imprimir cores e imagens do plano de fundo.

   As páginas da web do CA SDM incluem gráficos de fundo.

Para imprimir páginas da Web do CA SDM no Firefox

1. Selecione Arquivo, Configurar página.
2. Selecione a guia Format & Options.
3. Marque a caixa de seleção Print Background (color & images).

   As páginas da web do CA SDM incluem gráficos de fundo.

Modificação de arquivo de configuração

Quando você instala a interface web do CA SDM, um arquivo de exemplo de configuração do mecanismo web (*web.cfg*) é instalado, o qual pode ser modificado para atender às suas necessidades. O próprio arquivo *web.cfg* contém comentários úteis que você pode ler ao visualizar o arquivo. É possível abrir o arquivo *web.cfg*, a partir do diretório apropriado:

- (Windows) %NX_ROOT%\bopcfg\www\
- (UNIX) $NX_ROOT/bopcfg/www/

Observação: algumas variáveis adicionais de configuração, como conjunto de caracteres, também estão disponíveis no Gerenciador de opções. Elas podem ser acessadas usando a guia Administração na interface web. Para obter mais informações, consulte a *Ajuda online*.

AllowInactiveSrelEntry

Especifica se um registro pode ou não ser salvo quando ele se refere a registros inativos em uma tabela de referência.

- Quando essa propriedade é omitida ou definida como zero, as entradas inativas da tabela de referência (como o status de solicitação ou a categoria de mudança) não são incluídas nas seleções suspensas e não podem ser especificadas para os campos de pesquisa hierárquica ou consulta.
- Quando essa propriedade é definida como 1, o sinalizador inativo é ignorado nas entradas da tabela de referência.

Independentemente da configuração desse sinalizador, os registros que já contêm uma referência a uma entrada inativa da tabela de referência podem ser salvos sem alterar a referência; o sinalizador afeta apenas os novos valores do campo.

AnnouncementLength

Especifica o número máximo de anúncios a serem exibidos na tela de abertura tanto para a interface do cliente quanto para a interface do analista. O CA SDM começa a exibição com o anúncio mais recente, continuando para o número de anúncios especificado por este parâmetro. Os usuários da interface do analista podem visualizar anúncios adicionais selecionando Anúncios no menu Pesquisar.

Padrão: 10, significando que os 10 anúncios mais recentes são exibidos.

AnonymousPrio

Especifica as prioridades válidas para tickets criados pelos usuários convidados. Tais usuários podem especificar apenas uma das prioridades na lista AnonymousPrio para seus tickets. As entradas na lista de prioridades são separadas por espaços. Cada entrada deve ser um número entre 1 e 5 ou a palavra “nenhum” (sem aspas). A prioridade padrão para tickets criados por usuários convidados deve ser especificada primeiro e pode ser repetida na lista.

Os valores válidos para AnonymousPrio correspondem aos nomes simbólicos das prioridades conforme a distribuição. Você pode usar o cliente Java para personalizar esses nomes simbólicos; no entanto, isso não afeta a especificação para AnonymousPrio, que deve continuar para fazer referência às prioridades por seus nomes padrão, em que 1 corresponde à prioridade mais alta.

Padrão: nenhum, significando que todas as solicitações criadas por um usuário convidado têm uma prioridade de nenhum.

Preenchimento automático

Especifica que a interface da Web deveria preencher automaticamente os campos de pesquisa quando um usuário digita dados neles e pressiona a tecla Tab para sair do campo. Quando um usuário faz isso e a opção Preenchimento automático está selecionada, o navegador pede que o servidor confirme que a atualização está correta. Isso resulta no preenchimento do nome completo no campo (se o usuário forneceu um nome parcial) ou no aparecimento de uma janela de pesquisa pop-up (se a seleção do usuário estiver incorreta ou for ambígua).

Essa propriedade é opcional. O Preenchimento automático está ativado por padrão, portanto, se essa ID da propriedade for omitida ou definida como Sim, sair de um campo de pesquisa com tab automaticamente pesquisa no banco de dados. Se essa propriedade for definida como Não, não ocorrerá o preenchimento automático e os campos de pesquisa não são verificados até que o registro seja salvo.

CAisd

Especifica o caminho (incluindo uma barra no início) para o alias ou para o diretório virtual no servidor HTTP que contém os arquivos necessários pelo servidor web do CA SDM. Essa propriedade normalmente tem um valor /CAisd tanto nas instalações do UNIX quanto do Windows. Para os servidores Apache, deve ser definido em uma instrução Alias em um arquivo de configuração. Para o IIS, deve corresponder a um campo Alias na Janela Propriedades do diretório.

CGI

Especifica o nome do programa executável CGI fornecido com a interface da Web (sem o sufixo .exe).

Padrão: pdmweb

Observação: se renomear este programa, é necessário atualizar esta propriedade.

CgiReport

Especifica o nome do programa executável CGI para relatórios da Web fornecidos com a interface da Web (sem o sufixo .exe).

Padrão: pdm_cgireport

Observação: se renomear este programa, é necessário atualizar esta propriedade.

ContactAutoDesc

Especifica se o nome do contato deve ser inserido na descrição de novas ocorrências e solicitações criadas nas interfaces do cliente e do funcionário. Se essa propriedade for omitida ou especificada como 0, nenhuma informação automática será adicionada à descrição de novas ocorrências e solicitações. Se essa propriedade for especificada como 1, o nome do contato será automaticamente inserido na descrição de ocorrências e solicitações criadas nas interfaces do cliente e do funcionário. Esta propriedade não tem nenhum efeito na interface do analista.

ContactAutoDescWithIP

Especifica se o endereço IP do contato deve ser inserido na descrição de novas ocorrências e solicitações criadas nas interfaces do cliente e do funcionário. Se essa propriedade for omitida ou especificada como 0, nenhuma informação de endereço IP será adicionada à descrição de novas ocorrências e solicitações. Se essa propriedade e a propriedade ContactAutoDesc forem especificadas como 1, o nome do contato e o endereço IP serão automaticamente inseridos na descrição de ocorrências e solicitações criadas nas interfaces do cliente e do funcionário. Esta propriedade não tem nenhum efeito na interface do analista. Ignorada a menos que ContactAutoDesc seja 1.

CstPrio

Prioridades válidas para ocorrências criadas com a interface da Web do cliente. Os usuários da interface do cliente só podem especificar uma das prioridades na lista CstPrio para suas ocorrências e não podem atualizar a prioridade de uma ocorrência se um analista a alterou para um valor que não está na lista.

As entradas na lista de prioridades são separadas por espaços. Cada entrada deve ser um número entre 1 e 5 ou a palavra “nenhum” (sem aspas). A prioridade padrão para as ocorrências criadas com a interface do cliente deveria ser especificada primeiro (e pode ser repetida na lista).

Padrão: nenhum, 3, 4, 5

Os valores válidos para CstPrio correspondem aos nomes simbólicos das prioridades, conforme a distribuição. Você pode usar o cliente Java para personalizar esses nomes simbólicos; no entanto, isso não afeta a especificação para CstPrio, que deve continuar fazendo referência às prioridades por seus nomes padrão, em que 1 corresponde à prioridade mais alta.

DateFormat

Define a ordem de elementos em datas.

Padrão: DD/MM/YYYY hh:mm:ss

Símbolo	Descrição
m	Imprimir 1 ou 2 dígitos de mês
MM	Imprimir 2 dígitos de mês
D	Imprimir 1 ou 2 dígitos de data
DD	Imprimir 2 dígitos de data
YY	Imprimir 2 dígitos de ano
YYYY	Imprimir 4 dígitos de ano
h	Imprimir 1 ou 2 dígitos de horas no formato de 24 horas
HH	Imprimir 2 dígitos de horas no formato de 24 horas
h	Imprimir 1 ou 2 dígitos de horas no formato de 12 horas
hh	Imprimir 2 dígitos de horas no formato de 12 horas
m	Imprimir 1 ou 2 dígitos de minutos
mm	Imprimir 2 dígitos de minutos
s	Imprimir 1 ou 2 dígitos de segundos
ss	Imprimir 2 dígitos de segundos
a(am, pm)	Imprimir am e pm como uma seqüência

DateFormatNoTime

Especifica a mesma definição que DateFormat, mas sem especificar a porção de tempo.

DebugSource

Ativa o menu de clique com o botão direito do mouse do navegador padrão em formulários do CA SDM. Quando essa propriedade não está definida, você pode clicar com o botão direito do mouse em um formulário para exibir um menu do CA SDM. Você deve ter cuidado ao definir essa propriedade, uma vez que algumas das opções no menu acessado com um clique no botão direito do mouse do navegador padrão podem causar erros de execução (motivo pelo qual ela normalmente está desativada). No Internet Explorer, você pode exibir o menu acessado com um clique no botão direito do mouse do navegador padrão embora a propriedade DebugSource não seja definida pressionando a tecla CTRL quando você clica com o botão direito do mouse.

DebugTrace

Faz o mecanismo da web gravar informações de rastreamento para o arquivo stdlog.

Importante: Essa propriedade *não* deve ser definida para uso típico. Deve ser usada somente quando solicitada pelo Suporte da CA.

EmpPrio

Prioridades válidas para solicitações criadas com a interface da Web do funcionário. Os usuários da interface do funcionário só podem especificar uma das prioridades na lista EmpPrio para suas solicitações e não podem atualizar a prioridade de uma solicitação se um analista a alterou para um valor que não está na lista.

As entradas na lista de prioridades são separadas por espaços. Cada entrada deve ser um número entre 1 e 5 ou a palavra “nenhum” (sem aspas). A prioridade padrão para solicitações criadas com a interface do funcionário deve ser especificada primeiro (e pode ser repetida na lista).

Padrão: nenhum, 3, 4, 5

Os valores válidos para EmpPrio correspondem aos nomes simbólicos das prioridades conforme a distribuição. Você pode usar o cliente Java para personalizar esses nomes simbólicos; no entanto, isso não afeta a especificação para EmpPrio, que deve continuar fazendo referência a prioridades por seus nomes padrão, em que 1 corresponde à prioridade mais alta.

ExclLockSeconds

Especifica o número máximo de segundos durante os quais um usuário tem o bloqueio exclusivo sobre um registro depois de clicar em Editar. Depois que esse período termina, o mecanismo da Web libera o bloqueio, permitindo que outros usuários atualizem o registro. O mecanismo da Web tenta bloquear novamente se um usuário pedir para salvar depois que ExclLockSeconds tiver expirado. Essa tentativa progride apenas se nenhum outro usuário atualizou o registro enquanto o bloqueio estava disponível. Se a tentativa de bloquear novamente falhar, o usuário deverá inserir novamente as atualizações.

Padrão: 120 (dois minutos)

Esse argumento é opcional. Se omitido, o valor padrão é presumido.

Observação: a configuração de ExclLockSeconds deve ser mais curta que a definição de Timeout. ExclLockSeconds é especificado em segundos e TimeOut é especificado em minutos.

FormCacheMax

Especifica o número máximo de formulários a serem retidos na memória do mecanismo da Web para cada usuário. O mecanismo da Web sempre retém os últimos formulários de FormCacheMax usados por cada usuário. Formulários além desse número são elegíveis para serem expirados. Os formulários expirados não podem ser acessados pelos botões Voltar ou Avançar na página principal e não podem mais ser enviados em um formulário pop-up.

Padrão: 10

Os formulários expirados salvam a memória no mecanismo da Web, mas eles ocasionalmente exigem que os usuários façam a atualização manualmente. Você pode definir FormCacheMax como –1 para desativar o recurso FormTimeout.

FormTimeout

Especifica o número mínimo de segundos que um formulário é retido no mecanismo da Web antes de estar qualificado para remoção do cache. Os usuários sempre têm pelo menos o número de segundos especificado neste parâmetro para trabalhar em um formulário antes de enviá-lo. Além disso, o mecanismo da Web sempre mantém os formulários de FormCacheMax usados recentemente para cada usuário.

Você pode usar a propriedade StayCacheList para evitar que os formulários especificados expirem.

Padrão: 180 (3 minutos)

FormTitle

Especifica uma sequência de caracteres a ser incluída na barra de título de um navegador da Web que está exibindo um formulário da Web do CA SDM. O valor de FormTitle completa o título do formulário específico exibido.

Padrão: CA SDM

Por exemplo, se o valor padrão for mantido e o Microsoft Internet Explorer for usado para exibir o formulário Detalhes do anúncio, a barra de título exibe o seguinte:

Detalhes do anúncio—CA SDM— Microsoft Internet Explorer

Essa propriedade é opcional. Se for omitida, a interface da Web do analista não usará um valor de constante no título. As interfaces da Web do cliente e PDA revertem voltam para o valor padrão.

HitTrackFile

Especifica o caminho completo para um arquivo que recebe um log de todas as páginas da Web usadas. Uma linha é gravada nesse arquivo toda vez que um usuário solicitar uma página. O arquivo pode crescer indefinidamente, portanto, seja cuidadoso ao especificar essa propriedade.

Observação: os registros que contêm uma marca de data e hora, ID de usuário, ID de registro de banco de dados e nome do formulário HTPML são anexados a esse arquivo. O formato dos registros pode ser alterado. Periodicamente, você deve dar manutenção a esse arquivo para que ele não fique grande demais.

Essa propriedade é opcional. Se for omitida, nenhuma tentativa de rastreio do arquivo será gravada.

HtmplCacheSize

Especifica o tamanho do cache de HTPML. Quando esse tamanho é excedido, o formulário menos usado é removido do cache.

Padrão: 1000.

ListAllMaximum

Especifica o número máximo de registros que podem ser exibidos em uma lista antes que uma solicitação para exibir a lista inteira produza uma mensagem de aviso pop-up advertindo o usuário de que a solicitação causa um impacto negativo no desempenho e não é permitido.

Padrão: 2500

ListAllWarn

Especifica o número máximo de registros que podem ser exibidos em uma lista antes que uma solicitação para exibir a lista inteira produza uma mensagem de aviso pop-up advertindo o usuário de que a solicitação pode causar um impacto negativo no desempenho e pedindo a confirmação.

Padrão: 1000

ListBottomMaximum

Especifica o número máximo de registros que podem ser exibidos em uma lista antes que uma solicitação para rolar até a parte inferior produza uma mensagem de aviso pop-up advertindo o usuário de que a solicitação causa um impacto negativo no desempenho e não é permitida.

Padrão: 2500

ListBottomWarn

Especifica o número máximo de registros que podem ser exibidos em uma lista antes que uma solicitação para rolar para a parte inferior produza uma mensagem de aviso pop-up advertindo o usuário de que a solicitação pode causar um impacto negativo no desempenho e pedindo confirmação.

Padrão: 1000

ListPageLength

Especifica o número máximo de registros encontrados a serem exibidos em uma página de lista depois de executar uma pesquisa.

Padrão: 10

LogoutURL

Especifica o URL completo de uma página da Web a ser exibida depois que um usuário efetua logoff do CA SDM. Essa propriedade é opcional. Se não for especificada, efetuar logout retornará ao formulário de logon.

Lr_Refresh

Especifica o intervalo de atualização do leitor de logs em segundos. Se essa propriedade não for zero, o Leitor de logs de notificação será atualizado automaticamente no intervalo especificado (com, no mínimo, trinta segundos).

Essa propriedade é opcional. Se for omitida, o leitor de logs será atualizado automaticamente a cada 5 minutos (um valor padrão de 300 segundos). Se essa propriedade for especificada como zero, o leitor de logs não será atualizado automaticamente.

MacroPath

Especifica uma lista de caminhos do diretório que o mecanismo da web procura para localizar os arquivos solicitados pela marca PDM_MACRO. Você pode especificar vários diretórios separados por espaços. Você pode incluir variáveis de ambiente nos nomes do diretório, colocando um cifrão como prefixo (por exemplo, $NX_ROOT). Tanto para o Windows quanto para o UNIX, separe os componentes do caminho com uma barra normal (/), não com uma barra invertida (\). Essa propriedade é obrigatória. Isso normalmente é definido da seguinte forma:

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound

Especifica o texto da mensagem a ser exibido em um campo quando uma chave do usuário para um campo de pesquisa é ambígua e o formulário de edição deve ser exibido novamente com uma lista de seleção suspensa. Essa propriedade é opcional; se for omitida, assumirá como padrão Várias correspondências.

MaxRecordsAutoSuggest

Especifica o número de registros que a sugestão automática exibe, quando a pesquisa a medida que digita ou a sugestão automática exibir sugestões de uma pesquisa.

Padrão: 25.

MaxSelectList

Especifica o número máximo de correspondências a serem exibidas na lista de seleção suspensa mostrada quando uma chave do usuário para um campo de pesquisa é ambígua e o formulário de edição deve ser exibido novamente. Se forem encontradas ainda mais correspondências, é exibida a mensagem especificada para Foram encontradas muitas correspondências.

MinCharsAutoSuggest

Especifica o número mínimo de caracteres a serem digitados nos campos de pesquisa, antes de a pesquisa a medida que digita ou a sugestão automática exibir sugestões.

Padrão: 3.

MouseoverPreviewDelayTime

Especifica o tempo de atraso, em milissegundos, entre mover o cursor do mouse sobre um link e quando a visualização automática é exibida.

Ao mover o mouse pelo link antes do tempo de atraso expirar, não é possível visualizar.

Padrão: 1000

NoMatchesFound

Especifica o texto da mensagem a ser exibida em um campo quando uma chave do usuário para um campo de pesquisa está incorreta e o formulário de edição deve ser exibido novamente. Essa propriedade é opcional; se for omitida, assumirá como padrão Nenhuma correspondência encontrada.

PreLogin Timeout

Especifica o número máximo de minutos pelo qual o mecanismo da Web mantém uma sessão ativa antes do logon. O mecanismo da Web inicia automaticamente uma sessão quando um usuário solicita um formulário de logon, antes de o usuário concluir o logon. Se o usuário não efetuar logon dentro do período de tempo especificado, o mecanismo da Web destruirá a sessão. Se o usuário efetuar logon posteriormente, o mecanismo da Web cria uma nova sessão transparente ao usuário.

Essa propriedade não tem nenhum impacto para o usuário final. Seu único objetivo é o desempenho—equilibrando o uso de memória do mecanismo da Web contra a sobrecarga de destruição e recriação de uma sessão. Essa propriedade é opcional; se for omitida, assumirá como padrão um minuto.

RedirectingURL

Especifica o URL que o WebDirector deve usar para enviar solicitações a esse mecanismo da Web. Essa propriedade especifica o URL completo do mecanismo da Web, incluindo http. Essa propriedade é obrigatória se você estiver usando o WebDirector. Do contrário, é ignorado.

SchedExpMaximum

SchedExpMaximum

Especifica o limite do número de eventos de programação que podem ser exportados de cada vez.

Padrão: 1000

Importante: O padrão é o máximo de exportações que o CA SDM pode tratar de cada vez. Aumentar este padrão pode causar instabilidade no sistema. Se tentar exportar mais que o valor especificado em SchedExpMaximum, será exibida uma mensagem recusando a solicitação de exportação

SelListCacheExclude

SelListCacheExclude

SelListCacheExclude especifica os nomes das fábricas (objetos) a serem excluídos do armazenamento em cache para as listas <PDM_SELECT>. Para melhorar o desempenho, o mecanismo da Web normalmente armazena em cache em sua própria memória o conteúdo de tabelas pequenas usadas nas listas <PDM_SELECT> (suspensas) e nas listas de pesquisas hierárquicas. Você pode desejar suprimir o armazenamento em cache para uma tabela se estiver usando restrições de partição de dados para especificar que usuários diferentes devam receber exibições diferentes da tabela. Além disso, a inclusão de tabelas no valor dessa propriedade elimina a necessidade para o mecanismo da Web para consultar sua contagem de registros na inicialização, melhorando consideravelmente o desempenho da inicialização. Essa propriedade é opcional. Se for especificada, deve conter um ou mais nomes do objeto separados por espaços.

SelListCacheMax

SelListCacheMax

Define o número máximo de registros em uma tabela que pode ser armazenado em cache no mecanismo da Web. O mecanismo da Web mantém o conteúdo inteiro das tabelas em ou abaixo do seu tamanho do cache na própria memória, melhorando seu desempenho na criação das listas <PDM_SELECT>, usando essas tabelas. A especificação de um valor mais alto para essa propriedade melhora o desempenho às custas de uso de memória.

Padrão: 10

SelListCacheMax é ignorado para tabelas usadas em listas de pesquisas hierárquicas, tal como categoria em solicitações, ocorrências e requisições de mudança. O mecanismo da Web sempre armazena o conteúdo inteiro de tabelas usadas em listas hierárquicas de pesquisa na própria memória. Se você tiver um grande número de valores em qualquer uma dessas tabelas, talvez você queira especificar a propriedade SelListCachePreload.

SelListCachePreload

Especifica uma ou mais tabelas a serem carregadas no cache selecionado do mecanismo da Web no momento da inicialização. As tabelas não especificadas nessa propriedade são carregadas na primeira vez em que forem usadas. Se SelListCacheMax for grande ou se você tiver um grande número de registros em uma lista hierárquica de pesquisa (como categoria), talvez você deseje especificar a tabela em SelListCachePreload. Isso evita um atraso no tempo de resposta na primeira vez que um usuário acessar um formulário usando a tabela.

A especificação da propriedade SelListCachePreload é uma lista separada por espaços em branco de nomes do objeto. Cada nome do objeto pode ser seguido por uma lista opcional de nomes de atributo entre parênteses. Os atributos especificados na lista são carregados no mecanismo da Web. Se nenhum atributo for especificado, apenas o nome comum e o valor rel attr do objeto são carregados. Isso é suficiente para seleções suspensas, mas pode não ser suficiente para pesquisas hierárquicas. Se você modificar os formulários de pesquisa hierárquica (hiersel_xx.htmpl, em que xx é um nome de objeto), certifique-se de que a propriedade SelListCachePreload especifica cada atributo usado no formulário. Se você omitir um atributo, o cache será recarregado quando o formulário for usado.

A propriedade SelListCachePreload é opcional. Se for omitido, nada será carregado no cache selecionado até que um usuário solicite um formulário usando a seleção suspensa ou uma pesquisa hierárquica.

```
chgcat(description owning_contract) chgstat crs isscat(description
owning_contract) issstat pcat(description cr_flag in_flag pr_flag
owning_contract) pri tskstat urg pcat_cr(description cr_flag in_flag pr_flag
owning_contract) pcat_pr(description cr_flag in_flag pr_flag owning_contract)
pcat_in(description cr_flag in_flag pr_flag owning_contract)
```

StayCacheList

Especifica os nomes de formulários que nunca são removidos do cache de formulários, independentemente do tempo pelo qual eles foram exibidos. Essa propriedade assegura que os quadros fixos em uma exibição em quadros permaneçam pelo tempo que a sessão durar. Pode ser usada com cuidado para fazer com que outros formulários sejam armazenados permanentemente em cache. O padrão é:

```
scoreboard.htmpl top_splash.htmpl buttons.htmp hiersel_admin_tree.htmpl
```

SuppressHtmplCache

Especifica que o mecanismo da Web deve reler todos os arquivos definindo o conteúdo de uma página cada vez que a página for solicitada. A análise de um arquivo HTMPL consome uma quantidade significativa de tempo de processamento do mecanismo da web e, normalmente, envolve a leitura de vários arquivos físicos (uma vez que a maioria das páginas usa marcas PDM_INCLUDE). O mecanismo da Web normalmente salva os arquivos analisados na própria memória de modo que as solicitações posteriores para a mesma página podem ser satisfeitas imediatamente. Isso melhora consideravelmente o desempenho, mas pode ser inconveniente para os usuários no processo de desenvolvimento de páginas novas ou atualizadas, uma vez que o mecanismo da Web deve ser reciclado para que as mudanças entrem em vigor.

Essa propriedade é opcional e não exige nenhum valor. Se for especificada, o mecanismo da Web não armazena em cache os arquivos analisados, e as mudanças nos arquivos HTMPL entram em vigor imediatamente. Por causa de seu impacto no desempenho, essa propriedade não deve ser especificada em um ambiente de produção.

SuppressLoginAndLogoutMsg

Especifica que o mecanismo da Web não deve registrar uma mensagem no arquivo de log do CA SDM cada vez que um usuário efetua logon ou logoff da interface da Web.

Essa propriedade é opcional. Se não for especificada, o mecanismo da Web registra uma mensagem cada vez que um usuário efetuar logon ou logout.

SuppressMacroCache

Especifica que o mecanismo da Web deve descartar todas as macros salvas cada vez que uma nova página for solicitada. O mecanismo da Web normalmente salva macros analisado na própria memória de modo que as solicitações futuras para o macro possam ser satisfeitas imediatamente. Isso melhora o desempenho, mas pode ser inconveniente para os usuários no processo de desenvolvimento de macros novas ou atualizadas, uma vez que o mecanismo da Web deve ser reciclado para que as mudanças entrem em vigor.

Essa propriedade é opcional. Se for especificada, o mecanismo da Web não armazenará em cache macros analisadas e as mudanças nas macros entram em vigor imediatamente. Por causa de seu impacto no desempenho, essa propriedade não deve ser especificada em um ambiente de produção.

Tempo de expiração

Especifica o número de minutos pelo qual uma sessão do usuário pode estar inativa antes de ser encerrada automaticamente, liberando todos os recursos do servidor.

Observação: a configuração de Timeout deve ser mais longa do que a configuração de ExclLockSeconds. ExclLockSeconds é especificado em segundos e TimeOut é especificado em minutos.

TooManyMatches

Especifica o texto da mensagem a ser exibido sob um campo quando uma chave do usuário para um campo de pesquisa é ambígua e o número de correspondências para a chave excede o valor de MaxSelectList. Essa propriedade é opcional; se for omitida, assumirá como padrão Foram encontradas muitas correspondências.

UpdatedAnnouncementsPopup

O intervalo no qual o navegador verifica se há um novo anúncio. Quando um novo anúncio é encontrado, ele é mostrado automaticamente em uma janela pop-up. O valor do intervalo está em minutos. Para reduzir o impacto no desempenho do navegador, recomenda-se definir essa variável a um valor maior que 5 (minutos).

UseDirector

Especifica quando o WebDirector está controlando esse mecanismo da web. A tabela a seguir define os possíveis valores:

Valor	Descrição
Não	O mecanismo da Web é independente do WebDirector. Esse é o valor padrão.
Sim	O WebDirector deve iniciar todas as sessões, incluindo o formulário de logon. Se um usuário tentar fazer uma conexão direta com o mecanismo da Web, ele pedirá uma referência ao WebDirector.
Afterlogin	O mecanismo da Web dá referência de uma sessão ao WebDirector depois de autenticar um usuário. Um mecanismo da Web configurado com UseDirector AfterLogin é responsável unicamente pela autenticação e é, assim, um candidato para o uso de soquetes de segurança (SSL) para obter segurança máxima.
BeforeLogin	O mecanismo da Web dá referência de uma sessão ao WebDirector antes de autenticar um usuário. Um mecanismo da Web configurado com UseDirectory BeforeLogin nunca exibe uma página de logon e nunca aceita uma senha de logon.

Essa propriedade é opcional. Se for omitida, o mecanismo da Web não usará o WebDirector.

UseNestedTabs

Especifica se deve-se exibir o controle sobre a guia aninhada nos formulários de detalhes.

Padrão: ativado

WebDirectorSlumpName

Especifica o nome do WebDirector que está atendendo esse mecanismo da Web. Essa propriedade é necessária apenas se você estiver executando mais de um WebDirector ou se você configurou seu WebDirector para usar um nome de slump que não seja o padrão de web:director.

Essa propriedade é opcional se você estiver usando o WebDirector. Do contrário, é ignorado.

WillingnessValue

Especifica a disposição desse mecanismo da web de aceitar sessões com base em uma escala de 0 a 10. Essa propriedade é usada somente se você estiver usando o WebDirector. Esse valor é significativo apenas em comparação com a aceitação de outros mecanismos da Web associados ao mesmo WebDirector. O WebDirector transfere as sessões a mecanismos da Web em proporção a seus valores de aceitação. Um mecanismo da Web com um valor de aceitação duas vezes o valor de outro mecanismo da Web, em média, atende duas vezes mais o número de sessões.

Um WillingnessValue igual a zero significa que o mecanismo da Web não aceita nenhuma sessão. Esse valor pode ser útil quando UseDirector é AfterLogin.

Essa propriedade é opcional se você estiver usando o WebDirector. Do contrário, é ignorado. Se for omitida, o mecanismo da Web definirá sua aceitação como 5.

WorkFrameTimeout

Especifica o número máximo de segundos pelo qual o mecanismo da Web espera por uma resposta a uma solicitação interna do servidor antes de concluir que houve falha na solicitação. Essa propriedade é usada para recursos da interface da Web do CA SDM, exigindo dados do servidor diferentes das páginas da Web normais. Isso inclui recursos como o preenchimento automático, carregando propriedades de categoria e atualizando as contagens de placar. As solicitações de Workframe ao CA SDM raramente falham. Contudo, as solicitações do workframe a outros servidores (como produtos integrados, como Gerenciamento de conhecimento) podem falhar se o servidor de destino não estiver sendo executado ou se um problema de rede impedir o acesso a ele. A propriedade WorkFrameTimeout especifica uma duração de tempo antes de considerar falha na solicitação e o workframe estar disponível para outras solicitações.

Observação: WorkFrameTimeout não é verificada, a menos que um workframe seja necessário e todos os workframes estejam em uso. Portanto, é muito provável que um servidor remoto tenha mais tempo que o especificado para WorkFrameTimeout para responder. O valor de WorkFrameTimeout é mínimo.

Essa propriedade é opcional. Se for omitida, o mecanismo da Web usará um tempo limite de workframe de 30 segundos.

Capítulo 10: Configurando atribuição automática

Esta seção contém os seguintes tópicos:

Atribuição automática (na página 449)
Relacionamentos de atribuição automática (na página 450)
Métodos de atribuição automática (na página 450)
Como começar a implementação da atribuição automática (na página 451)
Grupo e responsável padrão (na página 458)
Ativação da atribuição automática (na página 459)
Substituição da atribuição automática (na página 460)
Controles de atribuição (na página 461)
Registro de atividades (na página 464)
Ativar o Log de atividade para atributos adicionais (na página 465)
Rastreamento de atribuição automática (na página 465)
Consultas armazenadas (na página 466)
Como a atribuição automática atribui tickets (na página 466)
Como a atribuição automática atribui tarefas do fluxo de trabalho (na página 474)
Atribuições automáticas com base em item de configuração (na página 477)

Atribuição automática

A *atribuição automática* do CA SDM pode reduzir significativamente o tempo necessário para gerenciar tickets automatizando o processo de atribuí-los a analistas. Esta automação pode tornar as tarefas associadas com o balanceamento de cargas de trabalho e coordenação de programações de trabalho muito mais eficientes.

É possível configurar a atribuição automática para atribuir tickets com base nos seguintes fatores:

- Quais grupos de analistas trabalham em quais tickets ou tarefas
- Quando o trabalho deve ser realizado

- Quais locais atendem aos clientes afetados
- A carga de trabalho e a disponibilidade de cada analista
- O valor de um atributo de um item de configuração associado com o ticket

  Observação: a atribuição automática com base no item de configuração (na página 477) permite criar atribuições específicas de grupo somente para tickets de Solicitação/Incidente/Problema.

Você não precisa implementar a atribuição automática toda de uma vez. É possível desenvolver uma estratégia para implementá-la gradualmente. Por exemplo, é possível iniciar ativando-a somente para tipos de ticket, grupos de analistas ou locais selecionados.

Relacionamentos de atribuição automática

O processo de atribuição automática pode envolver muitos elementos do CA SDM. Os relacionamentos do elemento são os seguintes:

- As áreas e categorias se relacionam com grupos, locais e turnos de trabalho.
- Os grupos se relacionam com locais e turnos de trabalho.
- Os modelos de CA Workflow se relacionam com contatos

Para tornar a atribuição automática fácil de administrar, todos os relacionamentos podem ser mantidos pelos elementos relacionados. Por exemplo, ao relacionar um grupo de analista a uma categoria de mudança, é possível manter a associação a partir da página de Detalhe da categoria de mudança ou da página de Detalhe do grupo.

Métodos de atribuição automática

Os seguintes métodos básicos permitem atribuir tickets automaticamente:

Atribuição automática com base em local

Cria atribuições para todos os tipos de tickets com base no seguinte:

- Áreas e categorias relacionadas a grupos, locais e turnos de trabalho
- Grupos relacionados a locais e turnos de trabalho
- Modelos do CA Workflow relacionados a contatos

Observação: a atribuição automática com base em local é conhecida simplesmente como atribuição automática.

Atribuição automática com base em item de configuração

Cria atribuições de grupo para tipos de ticket de solicitação, problema e incide com base no seguinte:

- Áreas relacionadas a tickets que estejam associados a itens de configuração
- Atributos de itens de configuração usados para registrar informações de contato/grupo

A atribuição automática com base em local e a atribuição automática com base em item de configuração são opções mutuamente exclusivas, pois é possível selecionar somente um algoritmo para uso em uma dada área de solicitação/incidente/problema. A atribuição automática com base em local e a atribuição automática com base em item de configuração servem para atribuir tickets quando eles são criados; no entanto, a atribuição automática com base em item de configuração é diferente porque também reavalia as atribuições para um ticket sempre que a área ou item de configuração de um ticket de solicitação/incidente/problema são modificados. Se a atribuição automática com base em item de configuração for especificada, mas não gerar uma atribuição de grupo para um ticket com sucesso, a opção Area_Defaults é consultada para determinar se os valores padrão de Grupo e Responsável devem ser usados para atribuir o ticket.

Como começar a implementação da atribuição automática

Siga essas diretrizes para começar a implementação da atribuição automática para analistas e grupos de analistas selecionados:

1. Identifique uma ou mais áreas ou categorias para as quais deseja ativar a atribuição automática.

   Observação: para verificar as configurações de área e categoria de seu site, examine suas configurações na interface da Web do CA SDM. Para obter instruções, consulte a *Ajuda online*.

2. Por padrão, a atribuição automática é desativada. Ative-a somente para as áreas e categorias (na página 452) onde você quer usá-la.

3. Crie relacionamentos entre uma área ou categoria identificada e os grupos de analistas (na página 452) aos quais podem ser atribuídos tickets por essa área ou categoria.

4. Marque membros individuais dos grupos de analistas (na página 453) como disponíveis.

Áreas e categorias

Observação: ao configurar áreas e categorias, considere a configuração de responsáveis e grupos padrão (na página 458).

Para configurar a atribuição automática de tickets de solicitação, incidência e problema, use os seguintes controles na guia Atribuição automática da página de Detalhes da área de solicitação/incidente/problema:

- Atualizar grupos
- Atualizar locais
- Atualizar turnos de trabalho

Observação: a caixa de seleção para ativar a atribuição automática também está localizada na guia Atribuição automática de cada uma daquelas páginas. Ela é visível somente enquanto a página estiver em modo de edição.

As seguintes páginas na interface fornecem os mesmos controles para configuração da atribuição automática para requisições de mudança e ocorrências:

- Detalhes da categoria de mudança
- Detalhes da categoria de ocorrência

Grupos de analista

Para configurar a atribuição automática é preciso, no mínimo, definir os relacionamentos entre grupos de analista e áreas ou categorias. Os responsáveis são escolhidos em grupos que atendam a *todos* os critérios de atribuição automática especificados. Se nenhuma restrição adicional for definida, os tickets serão atribuídos automaticamente ao membro do grupo com menos tickets ativos.

Se nenhum grupo for associado à área, o responsável e o grupo padrão serão atribuídos. Se esses padrões não forem definidos, o ticket será deixado para atribuição manual.

É possível manter os relacionamentos entre grupos e áreas ou categorias na página de detalhes da área ou categoria.

Alternativamente, é possível manter os mesmos relacionamentos na guia Atribuição automática da página de Detalhes do grupo usando os seguintes controles:

- Atualizar áreas de solicitação
- Atualizar categorias de mudança
- Atualizar categorias de ocorrência
- Atualizar locais

Analistas

Campos na página Detalhe do analista determinam se o analista pode receber a atribuição automática.

Analistas podem receber atribuição automática somente se estiverem marcados como disponíveis.

A página de Detalhe do analista fornece uma caixa de seleção Disponível que ativa a atribuição automática.

Considere a hipótese de permitir que os analistas controlem sua própria disponibilidade para a atribuição automática. É possível monitorar a disponibilidade de analistas usando consultas armazenadas.

Observação: a caixa de seleção Disponível não é considerada durante a atribuição automática de tarefas de fluxo de trabalho.

O campo Programação de trabalho permite que os analistas tenham tickets atribuídos automaticamente somente durante seu turno de trabalho programado. Os analistas que não tenham programação de trabalho atribuída, mas estejam marcados como disponíveis, podem receber atribuição automática a qualquer momento, desde que não haja outras restrições que resultem em um status inelegível.

Como atribuir automaticamente tickets a um grupo e não aos contatos do grupo

A atribuição automática no CA SDM atribui tickets a contatos que têm a opção Disponível selecionada no registro de contato. No entanto, é possível atribuir automaticamente incidentes/problemas/solicitações/pedidos de alteração a um grupo e não aos contatos do grupo. A opção NX_AUTOASG_GROUP_ONLY controla o comportamento de atribuição automática para grupos. Instale essa opção para atribuir automaticamente tickets ao grupo em vez de contatos individuais. NX_AUTOASG_GROUP_ONLY não está disponível na interface da web; ele é instalado a partir do prompt de comando.

Para atribuir tickets automaticamente ao grupo e não a contatos individuais no grupo, Os campos a seguir precisam de explicação:

1. Verifique se a instalação do CA SDM está em um nível mínimo de correção cumulativa 2 do Release 12.7.
2. Abra o prompt de comando a seguir no servidor do CA SDM.
3. Execute o seguinte comando:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst
   ```

   Por padrão, as novas opções que você adicionar ao arquivo nx.env não serão salvas após executar pdm_configure. É possível salvar as alterações permanentemente especificando a opção -t, como a seguir:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst -t
   ```

   Os comandos atualizam os seguintes arquivos no CA SDM com a nova opção:

   - Windows—NX_ROOT/NX.env e NX_ROOT\pdmconf\nx.env.nt.tpl
   - UNIX/Linux—NX_ROOT/pdmconf/NX.env.tpl
4. Abra o arquivo NX.env na pasta de instalação do CA SDM e pesquise pela variável @ NX_AUTOASG_GROUP_ONLY=1 (localizada no final do arquivo).
5. Abra o arquivo nx.env.nt.tpl presente em NX_ROOT/pdmconf e pesquise pela opção @NX_AUTOASG_GROUP_ONLY=1.
6. Reinicie o serviço do Servidor de Daemon do Unicenter ServiceDesk.

   O CA SDM atribui tickets automaticamente apenas para o grupo.

Atribuição automática por local

Se sua área de serviço é grande e consiste em muitos locais que prestam serviços a diferentes comunidades de clientes, você pode usar o local como um fator em sua configuração de atribuição automática, como segue:

- **Local atribuído a uma área ou categoria** — Se você atribuir um local a uma área ou categoria, os tickets nessa área ou categoria serão atribuídos automaticamente apenas se um local correspondente for encontrado. Por exemplo, um ticket de solicitação será atribuído automaticamente se houver um analista qualificado nos seguintes locais:

  1. Local do ativo afetado
  2. Local do cliente afetado

  Se o ativo ou cliente afetado não tiver local especificado, a solicitação será atribuída ao grupo ou responsável padrão. Se esses padrões não forem definidos, a solicitação será deixada para atribuição manual. É possível usar as páginas de detalhe de área ou categoria para manter relacionamentos entre locais e áreas ou categorias.

- **Local atribuído a grupo** — Se você associar um local a um grupo, somente os membros desse grupo estarão qualificados para atribuição automática dos tickets que pertencem ao local. É possível usar páginas de detalhes de grupo para manter relacionamentos entre grupos e locais.

Para manter relacionamentos de local com áreas, categorias ou grupos, use os seguintes controles na guia Atribuição automática da página Detalhes do local:

- Atualizar áreas de solicitação
- Atualizar categorias de mudança
- Atualizar categorias de ocorrência
- Atualizar grupos

Exemplos: usar local na configuração de atribuição automática

Os seguintes exemplos mostram como é possível usar locais em sua configuração de atribuição automática:

- **Atribuir automaticamente tickets somente em um local especificado** — Os tickets de outros locais recebem o responsável e grupo padrão ou são deixados para atribuição manual. Por exemplo, você pode ter muitos usuários na sede da empresa e grupos menores de usuários em escritórios regionais. Um grupo de analistas alocado na sede atende os usuários locais, enquanto grupos de analistas móveis visitam os escritórios regionais. Você pode configurar a atribuição automática de tickets somente para os analistas da sede e atribuir tickets manualmente aos analistas móveis.
- **Atribuir tickets automaticamente por usuário ou local de ativo** — Você pode restringir a qualificação à atribuição automática aos grupos de analistas em locais que correspondam ao local do usuário ou ativo afetado. Por exemplo, sua organização pode ter muitos escritórios, e os tickets de cada escritório podem ser manipulados somente pelos grupos localizados naquele escritório. É possível relacionar cada grupo a áreas ou categorias apropriadas *e* ao local apropriado. A lógica da atribuição automática seleciona os analistas qualificados somente dos grupos do local correto.

Atribuição automática por turno de trabalho

Você pode impor a atribuição automática relacionando uma área ou categoria a um turno de trabalho. O turno de trabalho determina o intervalo de tempo dentro do qual os tickets se qualificam para atribuição automática. Os tickets abertos fora do horário do turno de trabalho são atribuídos ao analista e grupo padrão ou deixados para atribuição manual.

Também é possível usar turnos de trabalho para controlar a elegibilidade de grupos e analistas para a atribuição:

- Se você atribuir uma programação de trabalho a um grupo, analistas naquele grupo são elegíveis para atribuição automática somente para tickets abertos durante sua programação de trabalho.

  Observação: o turno de trabalho de um grupo é especificado no campo Programação de trabalho na página de Detalhes do grupo.

- Se você atribuir uma programação de trabalho a um analista individual, o analista será elegível para atribuição automática somente para tickets abertos durante aquela programação de trabalho.

  Observação: o turno de trabalho de um analista é especificado no campo Programação de trabalho na página de Detalhes do analista.

Durante a criação do ticket, a lógica de atribuição automática tenta identificar o analista com o menor número de tickets ativos em um grupo que atenda aos critérios de elegibilidade da atribuição. Se um analista apropriado não for identificado, o ticket é atribuído ao grupo e responsável padrão. Se esses padrões não forem definidos, o ticket será deixado para atribuição manual.

Para tarefas de fluxo de trabalho associadas a requisições de mudança ou ocorrências, a atribuição automática usa uma estratégia mais simples de seleção. Os responsáveis são selecionados a partir de grupos associados a modelos de fluxo de trabalho. Os responsáveis de tarefas de fluxo de trabalho podem ser de qualquer tipo de contato, exceto grupo. Quando uma tarefa muda para o status pendente, a atribuição automática seleciona o contato que tem o menor número de tarefas de requisições de mudança ou de fluxo de trabalho atribuídas. Para prevenir resultados indesejados, se a categoria de requisição de mudança ou a categoria de ocorrência pai não estiver ativada para atribuição automática, as tarefas não serão atribuídas automaticamente. Como as tarefas de fluxo de trabalho poderiam potencialmente incluir indivíduos externos à organização da central de serviços, contar com eles para refletir precisamente a disponibilidade com o sinalizador disponível poderia ser problemático.

Observação: a atribuição automática de tarefas de fluxo de trabalho não avalia o sinalizador, e não está disponível para categorias configuradas usando o processamento do CA Workflow.

É possível usar as páginas de detalhe da área ou da categoria para relacionar um turno de trabalho a uma área ou categoria, ou usar os seguintes controles na página de Detalhes do turno de trabalho:

- Atualizar áreas de solicitação
- Atualizar categorias de mudança
- Atualizar categorias de ocorrência

Exemplos: usar turnos de trabalho na configuração de atribuição automática

Os seguintes exemplos mostram como é possível usar turnos de trabalho em sua configuração de atribuição automática:

- **Atribuir tickets automaticamente ao turno em horário de trabalho** — Se seu service desk operar 24 horas por dia, você poderá configurar a atribuição automática para que os problemas de interrupção de rede sejam atribuídos ao turno que estiver em horário de trabalho quando o ticket for aberto.
- **Permitir atribuição automática somente durante um turno especificado** — Você pode impor a atribuição automática de tickets em algumas áreas ou categorias. Por exemplo, se os analistas de aplicativo de um local estiverem trabalhando somente durante o turno do dia, é possível atribuir automaticamente problemas de aplicativos somente durante este turno.

Grupo e responsável padrão

Quando a lógica de atribuição automática que você definiu for incapaz de identificar um grupo ou responsável adequado, o ticket é atribuído ao grupo e responsável padrão. É possível especificar esses padrões nos campos Grupo e Responsável nas seguintes páginas de interface da web:

- Detalhes de área de solicitação/incidente/problema
- Detalhes da categoria de mudança
- Detalhes da ocorrência

Se a atribuição automática não puder identificar um grupo ou responsável adequado e os padrões não estiverem especificados, o ticket é deixado para atribuição manual.

Ativação da atribuição automática

As opções e controles permitem configurar a atribuição automática. É possível controlar se o processamento de atribuição automática ocorre da seguinte forma:

- Para solicitações, incidentes e problemas atribuídos àquela área, use a guia Atribuição automática ativada na página Detalhes da área de Solicitação/Incidente/Problema.
- Para requisições de mudança, ocorrências e tarefas de fluxo de trabalho, selecione a guia Atribuição automática e a caixa de seleção Atribuição automática ativada na página de Detalhes da categoria de mudança, página de Detalhes da categoria de ocorrência e páginas de Detalhes do modelo do CA Workflow.

Observação: clique em Editar para tornar a caixa de seleção Atribuição automática ativada visível.

Exemplo: ativar atribuição automática para uma área de solicitação/incidente/problema

Este exemplo demonstra como ativar a atribuição automática para uma área de solicitação/incidente/problema.

1. Na guia Administração, vá para Service Desk, Solicitações/incidentes/problemas, Áreas.

   A página Lista de área de solicitações/incidentes/problemas é exibida.

2. Clique na área para a qual deseja configurar a atribuição automática.

   A página Detalhes de área de solicitações/incidentes/problemas é exibida.

3. Clique em Editar.

   A página Atualizar área de solicitações/incidentes/problemas é exibida.

4. Selecione a guia Atribuição automática e preencha os campos da seguinte maneira:

   Modo de atribuição automática

   Especifique como atribuição automática ocorre. A opção Com base em item de configuração é usada para basear a atribuição automática sobre o valor Atributo de IC atribuível.

   - **Desativado**—Baseia a atribuição automática na opção Area Defaults quando é instalada.
   - **Com base em item de configuração**—Baseia a atribuição automática no valor do atributo de IC atribuível.
   - **Com base em local**—Baseia a atribuição automática no valor de local.

   Atributo de IC transferível

   Especifica o atributo do item de configuração para usar para a atribuição de grupo. É possível digitar um valor diretamente ou clicar na lupa para pesquisar um atributo.

5. Clique em Salvar.

   A área de solicitação/incidente/problema permite definir valores padrão inseridos automaticamente em tickets de solicitação, incidente ou problema atribuídos à área.

Substituição da atribuição automática

Você pode usar a opção de Substituição da atribuição automática (autoasg_override) no Gerenciador de opções para determinar se a atribuição automática substituirá um analista ou grupo que pode ter sido definido durante a criação de um ticket.

Outros recursos no CA SDM podem ter definido o responsável e/ou grupo antes de a atribuição automática obter controle. É possível personalizar seu sistema definindo essa opção para um dos seguintes valores:

0

Respeita o grupo e/ou responsável existente. O processamento da Atribuição automática não ocorrerá se o responsável e/ou grupo foi definido durante a criação do ticket.

1

Ignora o grupo e/ou responsável existente. O processamento da atribuição automática continuará tentando encontrar um responsável e/ou grupo.

Você pode definir o responsável e/ou o grupo de várias maneiras:

- Manualmente pelo Analista
- Padrões da área e opções de definição de Destinatário
- Modelos de solicitação
- Integração do CA NSM

Observação: desinstalar a opção Substituição da atribuição automática faz com que ele funcione no modo padrão, ou seja, 0.

Controles de atribuição

As opções e controles permitem configurar a atribuição automática. Os recursos do CA SDM podem afetar a atribuição, os campos de grupo ou ambos em um ticket antes que ocorra o processamento da atribuição automática. Recomendamos analisar os controles de atribuição antes de implementar a atribuição automática.

Atribuição manual

Ao criar um ticket, o analista pode selecionar manualmente o responsável e/ou o grupo.

Opção de definição de responsável

Por padrão, o CA SDM definirá automaticamente o usuário conectado como o destinatário da ocorrência se esse usuário for um analista. Uma opção do Gerenciador de opções, Assignee_set, permite controlar este comportamento. Geralmente, essa opção é instalada por padrão.

Iss assignee_set

A opção Iss assignee_set define automaticamente o usuário conectado como o responsável pela ocorrência se esse usuário for um analista. É semelhante ao Assignee_set, exceto que é para Ocorrências ao invés de Solicitações.

Area_Defaults

A opção Areas_Default determina o que acontece quando a área de solicitação é especificada em uma página de detalhes da solicitação. Essa opção permite definir o responsável e o grupo sempre que ocorrerem mudanças na área de solicitação. O responsável e grupo padrão da área de solicitação são usados, e o processamento ocorre antes do processamento da atribuição automática.

Essa opção não é instalada por padrão.

Observação: a opção Category_Defaults fornece funcionalidade similar para requisições de mudança. A opção Iss_Category_Defaults fornece funcionalidade similar para ocorrências.

Opções de responsável e grupo obrigatórias

Várias opções estão disponíveis no Gerenciador de opções para controlar a criação de tickets não atribuídos. Essas opções são globais no escopo. Elas afetam a criação de todos os tipos de tickets indicados, independentemente de a atribuição automática estar em vigor. Se a condição indicada não for satisfeita, o ticket novo ou atualizado não poderá ser salvo.

As seguintes opções controlam a criação de tickets sem um responsável especificado:

require_change_assignee

Aplicação: Change Order Mgr

Descrição: torna obrigatório o campo Responsável de um ticket de requisição de mudança

require_issue_assignee

Aplicação: Issue Mgr

Descrição: torna obrigatório o campo Responsável de um ticket de ocorrência

require_incident_assignee

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Responsável de um ticket de incidente

require_problem_assignee

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Responsável de um ticket de problema

require_request_assignee

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Responsável de um ticket de solicitação

As seguintes opções controlam a criação de tickets sem um grupo especificado:

require_change_group

Aplicação: Change Order Mgr

Descrição: torna obrigatório o campo Grupo de um ticket de requisição de mudança

require_issue_group

Aplicação: Issue Mgr

Descrição: torna obrigatório o campo Grupo de um ticket de ocorrência

require_incident_group

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Grupo de um ticket de incidente

require_request_group

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Grupo de um ticket de solicitação

require_problem_group

Aplicação: Request Mgr

Descrição: torna obrigatório o campo Grupo de um ticket de problema

Modelos

Você pode usar modelos para definir os valores em uma nova solicitação, requisição de mudança ou ocorrência. Responsável e Grupo estão entre os campos que podem ser afetados pelos modelos.

Interface do CA Network and Systems Management

Quando o CA NSM e o CA SDM estão integrados e você cria solicitações a partir de eventos do CA NSM, o parâmetro user_parms nas definições de regra de elaborador é passado à API de texto. O processo de elaborador do CA SDM (tngwriter) define seus próprios parâmetros de substituição para alterar o texto antes de enviá-lo à API de texto. A palavra-chave LOG_AGENT é adicionada ao final da entrada para definir o log_agent para a solicitação.

Observação: é necessário atualizar o arquivo Text_API.cfg para todos os campos adicionais que são passados dos Sistemas de gerenciamento de alertas do CA NSM para o CA SDM. Este arquivo é usado para integrações com serviços web, email e AHD.DLL.

Mais informações:

Palavras-chave (na página 512)

Registro de atividades

A Atribuição automática registra as informações como eventos no log de atividades de um ticket. O êxito ou a falha da atribuição automática é registrado, e qualquer anomalia que possa ter ocorrido durante o processamento.

Ativar o Log de atividade para atributos adicionais

A exibição dos logs de atividade altera os valores de atributo dos objetos. Objetos, como todos os tipos de ticket, tarefas de fluxo de trabalho clássico, Pesquisas, Contatos, Itens de configuração, descrevem o log de atividade. É possível ativar o log de atividade para atributos adicionais No WSP.

Observação: é possível exibir os atributos simples do log de atividade, incluindo cadeias de caracteres, inteiros, data, duração e tipos de SREL. Não é possível exibir os logs de atividade para os tipos de lista, como as QRELs e BRELs.

Siga estas etapas:

1. Abra o WSP e inicie o Designer de esquemas.
2. Selecione a tabela que você deseja modificar e adicione atributos adicionais.
3. Para cada atributo, adicione +AUDITLOG() para o campo UI_INFO definido pelo site.

   Importante: Quando você adiciona o sinalizador AUDITLOG, você também *deve* remover a função val_fieldupdate_site() para evitar duplicar os logs de atividades.

4. Salve e publique o esquema.
5. Abra o WSP novamente e adicione os novos atributos para os formulários de detalhes.
6. Abra o CA SDM e defina uma associação de atividade para atributos adicionais.
7. Teste suas mudanças.

   Por exemplo, abra uma instância previamente salva de objetos e modifique os atributos afetados para verificar se aparecem os logs apropriados de atividades.

Rastreamento de atribuição automática

Em uma implementação complexa de atribuição automática, a atribuição automática poderá não tomar as decisões esperadas. O rastreamento pode ser habilitado para ajudar a entender o fluxo de processamento. O rastreamento normalmente está desativado, mas quando é ativado, numerosas mensagens são gravadas nos arquivos stdlog em $NX_ROOT\log, descrevendo as várias decisões tomadas pela atribuição automática.

Por esse motivo, tenha cuidado ao implementar isso em uma instalação de alto volume, uma vez que o número de mensagens geradas pode fazer com que os arquivos de log cresçam e, eventualmente, fiquem ocultos. Em sistemas muito ativos, pode ocorrer a diminuição do desempenho. O rastreamento é controlado com o utilitário pdm_logstat. Os parâmetros usados por esse utilitário fazem distinção entre letras maiúsculas e minúsculas. Digite-os conforme a exibição.

Para ativar o rastreamento, execute o seguinte comando no servidor:

```
pdm_logstat –f auto.pm milestone
```

Para desativar o rastreamento, execute o seguinte comando no servidor:

```
pdm_logstat –f auto.pm
```

Consultas armazenadas

Duas consultas armazenadas são fornecidas para monitorar a disponibilidade dos analistas. Os gerentes do CA SDM podem adicioná-las a seus Gerenciadores de filas:

- **Analistas disponíveis**—Analistas que estão marcados como disponíveis para atribuição automática
- **Analistas indisponíveis**—Analistas que estão marcados como indisponíveis para atribuição automática

Como a atribuição automática atribui tickets

Atribuição automática atribui tickets da seguinte forma:

1. A operação de salvamento inicial de um novo ticket chama a atribuição automática.

   Se uma área ou categoria não for configurada para atribuição automática, o processamento é interrompido.

2. A atribuição automática determina se Autoasg_override é instalado.

   Se não estiver instalado e o ticket possuir um responsável ou grupo, o processamento é interrompido.

3. Se turnos de trabalho forem relacionados ao ticket, a data de abertura é avaliada para determinar se um turno de trabalho inclui o ticket.

   Se um turno de trabalho não incluir o ticket, o processamento é interrompido, e a atribuição automática tenta atribuir o grupo e o responsável padrão.

4. A atribuição automática determina se algum grupo está relacionado ao ticket.

   Se não houver grupos relacionados, o processamento é interrompido e a atribuição automática tenta atribuir o grupo padrão e o responsável.

5. A atribuição automática desconsidera quaisquer grupos com um turno de trabalho associado, em que a data de abertura estiver fora do intervalo de tempo do turno de trabalho. Os grupos sem turno de trabalho ignoram a filtragem.

6. Para os locais relacionados ao ticket, ocorre o seguinte:

   - Se este ticket for uma solicitação e possuir um item de configuração

     O local do item de configuração corresponde aos locais relacionados à área de solicitação. Se não ocorrer nenhuma correspondência, o processamento é interrompido e a atribuição automática tenta atribuir o grupo e o responsável padrão. Caso contrário, é feita a correspondência do local do cliente com os locais relacionados à área ou categoria. Se não ocorrer nenhuma correspondência, o processamento é interrompido e a atribuição automática tenta atribuir o grupo e o responsável padrão.

   - Se os Locais estiverem associados à área de solicitação ou categoria

     Se os Locais estiverem associados à área de solicitação e ao item de configuração (durante o processamento da atribuição automática da solicitação) ou o cliente não possuir nenhum local, a atribuição automática interrompe o processamento.

7. A atribuição automática desconsidera os grupos qualificados que têm locais relacionados que não correspondem ao local do item de configuração (apenas para as solicitações) ou ao local do cliente. Se não restar nenhum grupo, o processamento é interrompido e a atribuição automática tenta atribuir o grupo e o responsável padrão.

8. A atribuição automática cria uma lista de analistas de cada um dos grupos qualificados restantes.

9. Os analistas indisponíveis são desconsiderados.

10. Os analistas restantes são verificados quanto às Programações de trabalho. Os que tiverem Programações de trabalho serão desconsiderados se a Data de abertura não estiver dentro das programações de trabalho do analista.
11. Se não restar nenhum analista, o processamento é interrompido e a atribuição automática tenta atribuir o grupo e o responsável padrão.
12. Todos os analistas restantes são classificados de acordo com o número de tickets ativos atribuídos a eles.
13. O analista (e o grupo associado) com menor número de tickets ativos é atribuído ao ticket. Se houver empate, será escolhido o primeiro analista que aparecer no grupo.

Iniciar Atribuição automática
Sinalizador de substituição definido?
Sim
Não
Responsável já existe?
Sim
Mensagem de erro de log
"AHD05441 Ticket tem um responsável atribuído"
Sair
Não
Grupo já atribuído?
Sim
Mensagem de erro de log
"AHD05442 Ticket tem um grupo atribuído"
Sair
Não
Área/categoria de solicitação vazia?
Sim
Sair
Não
Há turnos de trabalho associados?
Não
Sim
Data de abertura dentro de algum turno de trabalho?
Não
Mensagem de erro de log
"AHD 05443 Não atendido neste período"
Atribuir grupo e responsável padrão de área de solicitação
Sair
Sim
Para página 2
PÁGINA
1 de 4

De página 1
Grupos associados?
Não
Mensagem de erro de log
"AHD 05444 Nenhum Grupo para atender este ticket"
Atribuir grupo e responsável padrão de área de solicitação
Sair
Sim
Localizar todos os grupos associados a esta área/categoria de solicitação
Filtrar grupos com turnos de trabalho associados que não satisfaçam a data de abertura do ticket
Lista de grupos qualificados
Locais associados?
Não
Sim
Para página 4
Localizar todos os locais associados
Para página 3
PÁGINA
2 DE 4

De página 2
Isto é uma Solicitação? Existe um ativo?
Sim
Não
O ativo tem um local?
Não
Sim
O cliente tem um local?
Sim
Não
Mensagem de erro de log
"AHD05450 Área de solicitação tem locais, mas Recurso afetado não tem nenhum Local"
Atribuir grupo e responsável padrão de área de solicitação
Sair
O local do ativo é atendido por esta área de solicitação?
Sim
Não
Mensagem de erro de log
"AHD05449 Nenhum Local de área de solicitação qualificado que atenda ao Local do Recurso afetado"
Atribuir grupo e responsável padrão de área de solicitação
Sair
O local do cliente é atendido por esta área/categoria de solicitação?
Sim
Não
Mensagem de erro de log
"AHD05447 Nenhum Local de área/categoria de solicitação qualificado que atenda ao Local do Usuário final"
Atribuir grupo e responsável padrão de área de solicitação
Sair
Mensagem de erro de log
"AHD05448 Área/categoria de solicitação tem locais, mas Usuário final afetado não tem nenhum Local"
Atribuir grupo e responsável padrão de área de solicitação
Sair
Lista de grupos qualificados
Filtrar grupos que não atendam o local do cliente ou ativo
Para página 4
PÁGINA
3 DE 4

De página 2
De página 3
Restam grupos qualificados nesta lista?
Não
Sim
Obter uma lista de analistas dos grupos qualificados
Mensagem de erro de log "AHD05453 Nenhum analista disponível encontrado"
Filtrar analistas com turnos de trabalho programados que não satisfaçam a data de abertura da solicitação
Atribuir grupo e responsável padrão de área de solicitação
Sair
Analistas disponíveis?
Não
Sim
Atribuir analista/grupo com a carga de trabalho mais baixa
Mensagem de erro de log "AHD05452 Nenhum Grupo qualificado encontrado que atenda este Ticket"
Chamar auto_site.pm para aceitar seleção
Atribuir grupo e responsável padrão de área de solicitação
Sair
Grupo/analista da mensagem de log atribuído
Sair
PÁGINA
4 DE 4

Como a atribuição automática atribui tarefas do fluxo de trabalho

A lógica de processamento é usada pela Atribuição automática para atribuir tarefas do fluxo de trabalho da seguinte maneira:

1. A atribuição automática é chamada quando o status de uma tarefa de fluxo de trabalho for alterado para pendente. Se o modelo de fluxo de trabalho a partir do qual a tarefa de fluxo de trabalho foi criada não estiver habilitado para atribuição automática, o processamento é interrompido. Se a categoria de requisição de mudança pai ou a categoria de ocorrência não estiver habilitada para atribuição automática, o processamento é interrompido.
2. A atribuição automática verifica se Autoasg_override está instalado. Se não estiver instalado e a tarefa possuir um responsável ou grupo, o processamento é interrompido.
3. O modelo de fluxo de trabalho a partir do qual a tarefa de fluxo de trabalho foi criada é verificado para ver se algum contato está associado a ele. Se não houver contatos, o processamento é interrompido.
4. A atribuição automática cria uma lista de todos os contatos que são membros dos grupos que estão associados atualmente ao modelo de fluxo de trabalho a partir do qual a tarefa de fluxo de trabalho foi criada. Quaisquer contatos nesta lista que forem grupos são desconsiderados.
5. Todos os contatos restantes são classificados de acordo com o número de tarefas de requisição de mudança ativas ou tarefas de ocorrência atribuídas a eles.
6. O contato e o grupo associado com o menor número de tarefas ativas são atribuídos à tarefa.

Iniciar Atribuição automática
Modelo ativado?
Não
Atribuir grupo e responsável padrão do modelo
Sair
Sim
Categoria Pai ativada?
Não
Atribuir grupo e responsável padrão do modelo
Sair
Sim
Sinalizador de substituição definido?
Sim
Não
Responsável já existe?
Sim
Mensagem de erro de log
"AHD05441 Tarefa tem um responsável atribuído"
Sair
Não
Grupo já atribuído?
Sim
Mensagem de erro de log
"AHD05442 Tarefa tem um grupo atribuído"
Sair
Não
Para página 2
PÁGINA
1 DE 2

De página 1
Grupos associados?
Não
Mensagem de erro de log
"AHD05444 Nenhum Grupo para atender a esta tarefa"
Atribuir grupo e responsável padrão do modelo
Sair
Sim
Obter todos os Contatos dos grupos associados ao modelo
Filtrar Contatos que são Grupos
Lista de responsáveis qualificados
Atribuir analista/grupo com a carga de trabalho mais baixa
Chamar auto_site.pm para aceitar seleção
Mensagem de log
Analista/grupo atribuído
Sair
PÁGINA
2 DE 2

Atribuições automáticas com base em item de configuração

A atribuição automática com base em item de configuração permite criar atribuições específicas do grupo que se aplicam a cenários específicos. É possível especificar que para tickets de Solicitação/Incidente/Problema abertos para uma Área específica, o valor de um atributo do item de configuração associado com o ticket controla sua atribuição.

As atribuições automáticas com base na localização e em item de configuração são opções exclusivas porque é possível selecionar apenas um algoritmo para uso em uma Área de Solicitação/Incidente/Problema. Ambos os modos de atribuições automáticas com base na localização e em item de configuração podem atribuir tickets quando são criados. No entanto, atribuições automáticas com base em item de configuração são diferentes porque elas reatribuem tickets sempre que uma Área de Solicitação/Incidente/Problema de um ticket ou item de configuração é alterada.

Exemplo: a Área de solicitação/incidente/problema atribui tickets a um grupo

Ao configurar a área de rede (para solicitações/incidentes/problemas) para realizar atribuições automáticas com base em item de configuração usando o atributo network_contact_uuid (operações de rede) como o valor Atributo de IC transferível, quaisquer tickets que estiverem abertos para a Área de rede são atribuídos automaticamente ao grupo especificado no campo Operações de rede do IC associado ao ticket. Se nenhum IC estiver associado ao ticket, ou se o valor do campo Operações de rede do IC estiver em branco ou não especificar um grupo, a atribuição não ocorre. Nesses casos, o sistema age de acordo com a opção Area Defaults do Gerenciador de opções, e atribui o ticket usando os campos Grupo e Responsável da Categoria.

Como funciona a atribuição automática com base em item de configuração

Tickets de solicitação/incidente/problema devem especificar o seguinte para que ocorra a atribuição automática com base em item de configuração:

- Um item de configuração e uma Área.
- A área deve ter a opção Atribuição automática definida como Com base em item de configuração.

Quando um analista cria atribui um ticket a essa Área, ou altera a Área em um ticket existente, o CA SDM examina o campo Atributo de IC atribuível da Área. O CA SDM usa o valor de Atributo de IC atribuível como o nome de um atributo e então tenta encontrar um atributo com um nome idêntico no item de configuração associado ao ticket. Se o atributo no item de configuração inclui um grupo, o ticket é atribuído a esse grupo.

O seguinte diagrama descreve o processo para atribuição automática com base em item de configuração em mais detalhes:

1. O CA SDM verifica o seguinte:
    a. A opção autoasg_override está definida?
    b. Um ticket especifica uma Área com sua Atribuição automática auto_assign_mode=2?
    c. A categoria especifica um atributo de IC atribuível?
    d. O ticket especifica um item de configuração?
    e. O item de configuração possui um valor de atributo de IC atribuível?
    f. O valor especifica um grupo no atributo do IC?
    g. O responsável de um ticket é um integrante do grupo de ticket?

2. Quando as respostas são positivas para todas as perguntas na etapa anterior, o CA SDM define o atributo de grupo do ticket para o atributo de grupo do IC, e registra a atribuição no log de atividade.

   Observação: o diagrama mostra como Atribuição automática com base em item de configuração usa a variável NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS para determinar se a opção Área está ativada. NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS é uma variável no arquivo NX.env, que está localizado no diretório $NX_ROOT\.

3. O CA SDM atribui o ticket ao grupo.

Início do processo
O autoasg_override está definido?
Não
O atributo de grupo do ticket já está definido?
Sim
Não
O ticket especifica uma categoria com um auto_assign_mode = 2?
Sim
A categoria especifica um atributo de IC transferível?
Atribuição de IC/categoria de log ignorada no log de atividades
Não
Sim
O ticket especifica um IC?
Não
A opção Area_Defaults está instalada e ativada?
Sim
Definir o atributo de grupo do ticket para o valor do grupo da categoria
Não
O IC tem um valor no atributo de IC transferível?
Sim
A opção NX_CHECK_ASSIGN_EE_IN_AREA_DEFAULT está ativada?
Não
Sim
O valor do atributo de IC transferível no IC especifica um grupo?
Sim
O responsável da categoria é integrante do grupo da categoria?
Sim
Definir o responsável do ticket para o valor do responsável da categoria
Definir o atributo de grupo do ticket para o grupo no atributo do IC
Não
Não
Não
O integrante responsável do ticket é do grupo do ticket?
Sim
Registrar a atribuição no log de atividades
Não
Não
Limpar o atributo de responsável do ticket
O atributo de responsável é necessário?
Sim
Cancelar a operação de salvamento
Processo concluído

Mais informações:

Substituição da atribuição automática (na página 460)

Habilitar atribuições automáticas com base em item de configuração

A atribuição automática com base em item de configuração permite criar atribuições específicas do grupo que se aplicam a cenários específicos. É possível especificar que para tickets de Solicitação/Incidente/Problema abertos para uma Área específica, o valor de um atributo do item de configuração associado com o ticket controla sua atribuição. Atribuição automática com base em item de configuração reatribui tickets sempre que a Área de Solicitação/incidente/problema de um ticket ou item de configuração é alterado.

Observação: a opção autoasg_override do Gerenciador de opções controla as circunstâncias em que a atribuição automática acontece. Quando essa opção é definida para 1, o CA SDM ignora quaisquer configurações existentes de responsável e grupo e atribui automaticamente tickets em todos os casos. Se você quiser que o CA SDM atribua tickets automaticamente somente quando eles ainda não estiverem atribuídos, defina o valor da opção como 0.

Para ativar a atribuição automática com base em item de configuração

1. Na guia Administração, navegue para Service Desk, Solicitação/incidente/problema, Áreas.

   A Lista de áreas de solicitação/incidente/problema aparece.

2. Clique na área a ser editada.

   A página Detalhes da área aparece.

3. Clique em Editar.

   A página Atualizar área aparece.

4. Selecione a guia Atribuição automática e preencha os campos como segue:

   Modo de atribuição automática

   Especifique como atribuição automática ocorre. A opção Com base em item de configuração é usada para basear a atribuição automática sobre o valor Atributo de IC atribuível.

Atributo de IC transferível

Especifica o atributo do item de configuração para usar para a atribuição de grupo. É possível digitar um valor diretamente ou clicar na lupa para pesquisar um atributo.

Clique em Salvar.

A atribuição automática é ativada. O CA SDM realiza atribuições automáticas com base em item de configuração usando o atributo especificado no campo Atributo de IC atribuível.

Capítulo 11: Gerenciando seu banco de dados

Esta seção contém os seguintes tópicos:

Utilitários de gerenciamento de banco de dados (na página 483)
Selecione e configure o banco de dados (na página 483)
Carregamento de banco de dados (na página 484)
Backup do banco de dados (na página 487)
Restauração do banco de dados (na página 487)
Substituição da tabela do banco de dados (na página 488)
Extração de dados (na página 488)
Retirada de referência de dados (na página 490)
Usar o modo Dbadmin (na página 493)
Regras de arquivamento e eliminação (na página 494)

Utilitários de gerenciamento de banco de dados

É possível executar utilitários para gerenciar seu banco de dados enquanto o CA SDM está desligado. se estiver executando utilitários de gerenciamento de banco de dados e estiver usando um banco de dados que não seja o repositório padrão do CA SDM, as variáveis de ambiente do banco de dados deverão ser definidas.

Observação: para obter informações sobre a definição de variáveis de ambiente, consulte a documentação do banco de dados que estiver usando.

Selecione e configure o banco de dados

Você pode selecionar o banco de dados e configurá-lo para uso do CA SDM.

Para selecionar e configurar um banco de dados

1. Selecione o banco de dados na lista suspensa Tipo de banco de dados e clique em Avançar.

   A página de configuração do banco de dados selecionado é exibida.

2. Digite as informações do banco de dados na página de configuração do banco de dados e clique em Avançar.

   A configuração do banco de dados está concluída.

   Observação: use o botão Ajuda nessa página para obter informações de configuração sobre os campos do banco de dados selecionado.

Os seguintes botões são exibidos nas páginas de configuração.

Ajuda

Para exibir a Ajuda para a página atual.

Cancelar

Para cancelar as configurações feitas até agora.

Voltar

Para voltar para a página anterior sem salvar nenhuma das mudanças feitas até agora na página atual.

Próximo

Para ir para a próxima página depois de salvar todas as mudanças feitas na página atual.

Carregamento de banco de dados

O utilitário de carregamento de banco de dados, pdm_userload, adiciona, atualiza e exclui registros do banco de dados do CA SDM. Crie um arquivo de entrada ASCII formatado para o utilitário pdm_userload e selecione as tabelas a serem carregadas e os campos opcionais a serem adicionados.

Importante: O utilitário pdm_userload acessa o banco de dados do CA SDM e não interage diretamente com os processos do software aplicativo. Os itens de inventário adicionados ao banco de dados com pdm_userload não atualizam as listas de auxiliares/seleção até que o aplicativo tenha sido parado e reiniciado.

Embora o utilitário pdm_userload possa ser executado com o aplicativo ativo, o desempenho do sistema é reduzido. Para obter melhores resultados, assegure que o servidor do CA SDM esteja sendo executado, mas que nenhum usuário esteja usando a interface de cliente antes de executar o pdm_userload.

Observação: se for necessário adicionar registros com campos de referência -cruzada, use o utilitário pdm_deref.

Mais informações:

Retirada de referência de dados (na página 490)

Como criar e usar um arquivo de entrada

É possível usar um arquivo de entrada e o utilitário pdm_userload para preencher tabelas de banco de dados.

O formato do arquivo de entrada é o seguinte:

- Coloque os valores de campo entre aspas duplas (“valor”) e separe os valores com uma vírgula e um espaço (“valor1”, “valor2”).
- coloque aspas duplas com uma barra invertida (\) para colocá-los nas seqüências de caracteres de texto. Para definir um campo de data/hora para a data e hora atual, use @NOW@ para o valor de entrada.
- Coloque cada registro entre chaves separadas por espaços, da seguinte maneira:

  ```
  ( { valores do campo de registro } )
  ```

- Se forem delimitados adequadamente, os registros de entrada podem ocupar mais de uma linha no arquivo de entrada contanto que campos individuais permaneçam em uma linha. Para um campo de várias linhas, como comentários, os valores podem incluir um novo caractere de linha (\n) para forçar uma nova linha quando o campo do banco de dados for exibido.
- Novos caracteres de linha explícitos são necessários apenas para formatação especial. O texto corrido comum é exibido automaticamente com quebras de linha apropriadas, como pode ser visto no exemplo a seguir:

  ```
  "O status do registro é \"COMPLETE\""
  ```

Para criar um arquivo de entrada para o utilitário pdm_userload, faça o seguinte:

1. Determine qual tabela você deseja carregar e os campos que deseja preencher nessa tabela.

   Você deve preencher o campo-chave Nome ou Símbolo para cada registro que você carregar.

2. Faça uma cópia do arquivo *filename*.dat para a tabela que está sendo carregada.
3. Edite sua cópia recém-criada do arquivo *filename*.dat, da seguinte forma:
   a. Adicione uma entrada para cada registro a ser carregado.
   b. Sob a linha TABLE (consulte o exemplo a seguir), remova os campos que não serão preenchidos.

      ```
      TABLE table_name
      fieldname1 fieldname4 . . . fieldnameN
      ```
4. Salve seu arquivo e saia do editor.
5. Execute o utilitário pdm_userload e especifique o arquivo, conforme mostrado no exemplo a seguir. Neste exemplo, o nome do arquivo de entrada é myData.dat:

   ```
   pdm_userload -f myData.dat
   ```

   A tabela do banco de dados é preenchida.

Mais informações:

pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)

Eliminar e restaurar restrições

Algumas tabelas mdb que começam com ca_ (como ca_contact_) têm restrições de referência que podem causar impacto no carregamento em massa dos dados, usando as ferramentas pdm_load, pdm_userload e pdm_restore. Se o carregamento em massa dessas tabelas for obrigatório, talvez você necessite eliminar as restrições de referência antes do carregamento em massa dos dados.

Dois scripts SQL são fornecidos para cada tipo de DBMS para eliminar e restaurar as restrições. Antes do carregamento em massa de dados que afetam as tabelas ca_*, execute a versão de Eliminação do script. Depois de concluir o carregamento de dados, execute a versão de Adição do script.

Para SQL Server, os scripts estão localizados em *diretório-instalação*\samples\views\SQLServer. Execute o seguinte comando para eliminar as restrições:

```
osql -E -e < SQLDropConstraints.sql'
```

Execute o seguinte comando para adicionar restrições retroativas:

```
osql -E -e < SQLAddConstraints.sql
```

Para Oracle, os scripts estão localizados em *diretório-instalação*\samples\views\Oracle.

Execute o seguinte comando para eliminar as restrições:

```
sqlplus mdbadmin/ <senha> < OracleDropConstraints.sql
```

Execute o seguinte comando para adicionar restrições retroativas:

```
sqlplus mdbadmin/ <senha> < OracleAddConstraints.sql
```

Backup do banco de dados

É possível fazer backup do conteúdo de uma única tabela de banco de dados, de várias tabelas de banco de dados ou do banco de dados inteiro do CA SDM usando o utilitário de backup de banco de dados pdm_backup. A saída do utilitário de backup é um arquivo ASCII que o utilitário pdm_restore pode usar.

como parte de seu processamento, pdm_backup primeiro fecha os daemons (Unix) ou serviços (Windows).

Mais informações:

pdm_backup--Gravar banco de dados no arquivo ASCII (na página 1149)

Restauração do banco de dados

O utilitário de restauração do banco de dados, pdm_restore, carrega um arquivo de saída pdm_backup no banco de dados do CA SDM. O utilitário pdm_restore primeiro desliga os daemons (UNIX) ou serviços (Windows). Em seguida, ele restaura, limpa e substitui todos os registros de banco de dados existentes. Use o arquivo no formato ASCII criado pelo pdm_backup como entrada para o utilitário pdm_restore.

Você também pode usar os utilitários pdm_restore e pdm_userload para obter acesso ao aplicativo CA SDM no caso de uma corrupção catastrófica do banco de dados. Se seu banco de dados estiver danificado de forma que você não posa obter acesso ao aplicativo e se todas as outras medidas falharam, execute novamente a configuração e reinicialize o banco de dados para recriar seu banco de dados e preencha os dados de referência e as tabelas do sistema.

Esse procedimento inicializa o banco de dados da mesma forma que você fez durante a instalação original. Agora você pode acessar o CA SDM. O utilitário pdm_restore pode ser usado para restaurar a última cópia de backup do banco de dados.

Mais informações:

pdm_restore--Restaurar um banco de dados (na página 1187)

Substituição da tabela do banco de dados

O utilitário pdm_replace é um meio fácil e rápido de substituir o conteúdo inteiro de uma tabela de banco de dados do CA SDM por novas informações. Este utilitário pode ser útil para grandes revisões de tabelas -de pesquisa.

Observação: o pdm_replace assume o mesmo formato de arquivo de entrada como pdm_userload. É possível criar um arquivo de entrada para pdm_replace usando pdm_extract; no entanto, você não pode usar a saída de pdm_backup como entrada para pdm_replace.

Mais informações:

Como criar e usar um arquivo de entrada (na página 485)
pdm_replace--Substituir uma tabela do banco de dados (na página 1184)

Extração de dados

O utilitário pdm_extract extrai dados do banco de dados do CA SDM e produz saída em diversos formatos. Esses dados podem ser processados posteriormente ou podem ser inseridos em outros aplicativos, como planilhas ou outro banco de dados.

Com o utilitário pdm_extract, é possível fazer o seguinte:

- Elimine o banco de dados inteiro do CA SDM
- Elimine uma ou mais tabelas de banco de dados
- Extraia informações específicas do banco de dados e produza a saída em um dos três formatos a seguir:
  - Saída compatível com pdm_userload
  - Saída CSV (Comma-separated value - Valor separado por vírgula)
  - Saída de estilo de relatório -informal

Mais informações:

pdm_extract--Extrair dados do banco de dados (na página 1162)

Usar o extrator de dados em UNIX

Antes de usar o extrator de dados do CA SDM no UNIX, você deve fazer o seguinte:

1. Defina o valor da variável de ambiente $NX_ROOT para o nome completo do caminho do diretório de instalação do CA SDM definido durante a instalação.
2. Acrescente $NX_ROOT/bin a sua variável de ambiente PATH.
3. Defina umask como 000.

Seleção de dados para extração

Para selecionar os dados para extração, o extrator de dados usa um subconjunto integral de SQL com as seguintes regras:

- Há suporte específico para as seguintes funções de SQL no subconjunto:
  - IS NULL, IS NOT NULL, LIKE
  - Instruções SELECT e cláusulas WHERE
- Não há suporte para o seguinte recurso de SQL no subconjunto:
  - Joins
  - Guias integradas e caracteres de- nova linha
  - Cláusulas diferentes de SELECT, FROM e WHERE

- Asteriscos (*) em instruções SELECT
- Instruções SELECT aninhadas
- Funções agregadas

- Todas as palavras do SQL reservadas devem estar em letras maiúsculas
- Cada token em uma cláusula WHERE deve estar cercado por um espaço branco
- Todas as especificações de data/hora devem estar em um dos três formatos:
  - Segundos decorridos de 12:00:00 da manhã, 1/1/1970 Horário de Greenwich (GMT):

    ```
    start_date< ou >174182431500
    ```

  - Formato DATE do SQL:

    ```
    start_date< or >DATE '2001-11-28'
    ```

  - Formato TIMESTAMP do SQL:

    ```
    start_date< or >TIMESTAMP '2001-07-04 15:45:00'
    ```

Observação: o formato TIMESTAMP usa GMT. É possível ajustar os fusos horários adicionando ou subtraindo o número apropriado de horas, como: 2001-03-23 14:00:00+02:00 ou 2001-06-06 04:45:00-09:00.

Retirada de referência de dados

O utilitário pdm_deref é uma ferramenta de retirada de referência que converte dados de várias origens em um formato adequado para carregamento no banco de dados do CA SDM. A retirada de referência extrai IDs internas para campos de -referência cruzada. O utilitário também pode ser usado para calcular o tempo inoperante e os valores de tempo inoperante do SLA.

O utilitário pdm_deref converte dados em um dos seguintes formatos:

- Saída compatível com pdm_userload, adequada para ser carregada no banco de dados do CA SDM
- Saída -CSV
- Saída de estilo de relatório -informal

Mais informações:

pdm_deref--Retirar referência dos dados ASCII (na página 1154)

Exemplo de como usar pdm_deref

O exemplo a seguir mostra como usar o utilitário pdm_deref em um sistema de acompanhamento de ticket do CA SDM.

Suponha que um sistema de rastreamento de ticket existente implementado em uma planilha tem colunas chamadas Descrição do problema, Nome e sobrenome do técnico e Data de entrada. Essas colunas correspondem aos campos descrição, responsável e open_date na tabela Change_Request do CA SDM. O campo Descrição do problema contém o mesmo tipo de dados que o campo Descrição. Mas o campo responsável é um campo numérico, enquanto o campo Técnico na planilha está no formato “sobrenome, nome”.

Para usar pdm_deref

1. Carregue os nomes dos técnicos na tabela Contato.
2. Prepare um arquivo de entrada pdm_deref com as informações existentes.
3. Crie um arquivo de especificações para mapear os novos nomes de contato para valores de responsável.
4. Prepare um arquivo de entrada pdm_userload a ser usado para atualizar a tabela Change_Request.

Esse processo é descrito com mais detalhes nas etapas a seguir:

1. Prepare um arquivo de entrada do pdm_userload, local.dat, para a tabela Location da seguinte forma:

```
TABELA ca.location
location_name address_2 address_2
{"Boulder NCC - NQ", "716 Main
    Street","Boulder, CO 84302"}
{"Colorado Springs NCC", "2765 Spring Street",
    "Colorado Springs, CO 84303"}
{"Denver NCC", "3765 Stoneridge Way", "Denver,
    CO 80254"}
```

2. Carregue os dados da seguinte forma:

```
pdm_load -f location.dat
```

3. Prepare um arquivo de entrada, contact.dat, com as informações originais da seguinte forma:

```
TABELA ca.contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank," "Harold", "NCC - HQ", "303-555-2333"}
{"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
```

4. Prepare um arquivo de especificações de ferramenta de retirada de referência, contact.spec, da seguinte forma:

```
Deref
{
output = location_uuid
output = location_uuid
rule = "SELECT id FROM ca.location WHERE location_name=?"
}
```

Importante: Não coloque um espaço em branco na frente da palavra-chave SELECT. O Deref usa os nomes e sobrenomes dos novos contatos para obter os campos ID numérico adequado para carregar a tabela Change_Request. Além disso, os “ganchos” representados por pontos de interrogação (?) correspondem aos campos de entrada especificados. Você deve ter o mesmo número de ganchos como campos de entrada e eles devem estar na mesma requisição.

5. Execute pdm_deref da seguinte forma:

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

O arquivo de saída, contact.out, é semelhante a:

```
TABELA ca.contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47",
"303-555-2333"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
"303-966-1987"}
{"Lyman", "Jeanie", "L.", "58AA42789957734E8BEE146D07F7AD49", "303-966-5301"}
```

6. Carregue o arquivo contact.out no banco de dados do CA SDM da seguinte forma:

```
pdm_load -i -f contact.out
```

Observação: é necessário usar o comando pdm_load para usar a opção –i.

7. (somente UNIX, opcional) Crie um script, Convert_Ticket, como mostrado a seguir:

```
#!/bin/sh
pdm_load -i $1
cat $2 | pdm_deref -s $3 | pdm_load -i
```

É possível executar esse script, como pode ser visto a seguir:

```
Convert Ticket location.dat contact.dat contact.spec
```

Neste exemplo, pdm_load com o -sinalizador i é usado para acelerar o processo. Se estiver fazendo essas atualizações regularmente, é possível descartar o -sinalizador i de modo que pdm_load verifique se existem registros duplicados

A seguir, exemplos adicionais dos arquivos de especificação de ferramenta de retirada de referência:

```
Deref
{
        {
        output = assignee
        rule = " SELECT id from ca.contact \
                WHERE first_name=? \
                AND last_name=? \
                AND middle_name=? "
}
```

Essa regra converte três campos rotulados como first_name, last_name e middle_name na UUID do contato apropriado. Se todos os três campos de entrada não estiverem presentes, a regra não será aplicada. Nenhuma correspondência gera uma mensagem de erro e o processamento continua. Para várias correspondências, o primeiro valor é usado; uma mensagem de erro é gerada e o processamento continua.

Usar o modo Dbadmin

O modo dbadmin é um utilitário que inicia a camada de manipulação de dados do sistema CA SDM sem iniciar a camada de objeto, o que permite bloquear todo o banco de dados para executar a manutenção de dados de nível mais baixo sem arriscar a integridade dos dados.

Por exemplo, você querer usar pdm_extract, pdm_load, pdm_deref e pdm_replace para executar atualizações de dados em lote no sistema. Usando o dbadmin, o administrador está, basicamente, bloqueando o banco de dados no sistema inteiro. Os utilitários de backup (pdm_backup) e de restauração (pdm_restore) bloqueiam automaticamente o sistema no modo sbadmin para garantir um backup e restauração consistentes.

O modo dbadmin também é útil se você personalizar o sistema sem iniciar a camada de objeto até que os dados sejam modificados. Por exemplo, tornar um atributo “obrigatório” em majic em um sistema existente pode confundir o animador se ele precisar atualizar um objeto que tem o atributo nulo obrigatório. Você pode colocar o sistema no modo dbadmin e atualizar os objetos usando pdm_load e, em seguida, iniciar o sistema como de costume.

Para colocar o sistema no modo dbadmin

1. Pare o CA SDM a partir de qualquer Gerenciador de serviços do Windows ou executando pdm_halt na linha de comando.

   Observação: é uma boa prática enviar um anúncio para alertar os usuários e verificar se há usuários conectados antes de parar o sistema.

2. Na linha de comando, digite o seguinte comando, usando as letras maiúsculas e minúsculas, como pode ser visto:

   ```
   pdm_d_mgr –s DBADMIN
   ```

   Observação: não há nenhuma mensagem de retorno, mas uma pausa ocorre antes de o prompt do comando retornar. Se não houver nenhuma pausa, verifique a ortografia para se certificar de que inseriu os dados corretamente.

3. Execute o pdm_status para verificar se o sistema está no modo dbadmin.

   Observação: quando o sistema está no modo dbadmin, ele retorna o seguinte status, indicando que é seguro trabalhar no sistema:

   ```
   C:\>pdm_status
   Os Daemons não estão sendo executados.
   ```

4. Quando todo o trabalho estiver concluído, execute o pdm_halt para encerrar o modo dbadmin.

5. Reinicialize o sistema seguindo os procedimentos normais.

Regras de arquivamento e eliminação

É possível definir as regras que deseja usar para executar os trabalhos de arquivamento e eliminação em seu banco de dados do CA SDM. Você pode modificar e ativar as regras existentes em vez de criar novas.

Importante: As regras padrão Arquivo morto e Purge são definidas como Inativo. É preciso definir o filtro de pesquisa para procurar por regras inativas. É possível executar uma regra selecionando-a no nó Regras de arquivamento e eliminação e clicando em Executar agora.

Exemplo: ativar a regra de log de auditoria

É possível ativar e executar a regra para arquivamento e eliminação de registros de log de auditoria.

Para ativar a regra de log de auditoria

1. Navegue até Arquivamento e eliminação, Regras de arquivamento e eliminação.

   A lista de regras de arquivamento e eliminação é exibida.

2. Clique em Mostrar filtro.

   Selecione Inativo na lista suspensa Status e clique em Pesquisar.

   As regras identificadas como Inativo são exibidas.

3. Selecione a regra Log de auditoria e clique em Executar agora.

   O processo de arquivamento e eliminação inicia para registros de log de auditoria.

   Observação: você pode editar a regra (na página 498) clicando no link Log de auditoria e em Editar.

Executar regras de arquivamento e eliminação

É possível executar regras de arquivamento e eliminação tanto ativas quanto inativas manualmente a qualquer momento.

Para executar uma regra de arquivamento e eliminação a partir da página Lista.

1. Na guia Administração, selecione Arquivamento e eliminação, Regras de arquivamento e eliminação na seção esquerda.

   A lista de regras de arquivamento e eliminação é exibida.

2. Selecione as regras que deseja executar clicando na caixa à esquerda do nome da regra, selecione o número de horas (1-24) após as quais deseja que a regra pare, e clique em Executar agora.

   Uma mensagem é exibida indicando que o processo de arquivamento e eliminação iniciou.

3. Clique em OK para fechar a caixa de mensagem.

Para executar uma regra de arquivamento e eliminação a partir da página Detalhes.

1. Na guia Administração, selecione Arquivamento e eliminação, Regras de arquivamento e eliminação na seção esquerda.

   A lista de regras de arquivamento e eliminação é exibida.

2. Selecione a regra desejada clicando no nome da regra.

   A página de detalhes da Regra de arquivamento e eliminação é exibida.

3. Selecione o número de horas (1-24) após as quais deseja que a regra pare e clique em Executar agora.

Exibir regras de arquivamento e eliminação

É possível visualizar as informações de resumo para cada regra de arquivamento e eliminação na página Lista de regras de arquivamento e eliminação. Para exibir essa página, selecione Arquivamento e eliminação, Regras de arquivamento e eliminação na seção esquerda na guia Administração.

Você pode configurar um filtro para exibir somente as regras correspondentes a certos critérios.

Pesquisar na Lista de regras de arquivamento e eliminação

Você pode configurar filtros para restringir a exibição de regras de arquivamento e eliminação a apenas aquelas correspondentes a determinados critérios.

Para filtrar a Lista de regras de arquivamento e eliminação

1. Clique em Mostrar filtro na página Lista de regras de arquivamento e eliminação.

   A parte superior da página exibe os campos de filtro.

2. Preencha os campos conforme o necessário para exibir somente as regras de interesse.

3. Clique em Pesquisar.

   A Lista regras de arquivamento e eliminação exibe as regras que corresponde aos critérios de filtro.

Iniciar arquivamento e eliminação usando um agendador de terceiros

Você pode usar um agendador de terceiros para iniciar e parar uma regra de arquivamento e eliminação. O programador deve oferecer suporte à emissão de comandos de uma linha de comando. O arquivo arcpur.frg está localizado no seguinte diretório:

$NX_ROOT\bopcfg\interp

Para iniciar arquivamento e eliminação com um agendador de terceiros

1. Abrir o agendador de terceiros.
2. Especificar a hora de início.
3. Execute o seguinte comando:
   ```
   bop_cmd -f arcpur.frg "start_arcpur('<rule_name>', 'hours')"
   ```
4. Especificar a hora de término.
5. Execute o seguinte comando:
   ```
   bop_cmd -f arcpur.frg "stop_arcpur('<rule_name>')"
   ```
   O arquivamento e a eliminação são programados.

Definições de regras de arquivamento e eliminação

É possível definir as regras que deseja usar para executar os trabalhos de arquivamento e eliminação em seu banco de dados do CA SDM. O produto fornece um conjunto de regras predefinidas de arquivamento e eliminação. Você pode escolher modificar e ativar as regras existentes em vez de criar novas.

Criar uma regra de arquivamento e eliminação

Você pode definir regras para arquivar automaticamente registros desatualizados e limpá-los do banco de dados.

Para criar uma regra de arquivamento e eliminação

1. Na guia Administração, selecione Regras de arquivamento e eliminação.

   A lista de regras de arquivamento e eliminação é exibida.
2. Clique em Criar.

   A página Criar Nova regra de arquivamento e eliminação aparece.

3. Preencha os campos conforme apropriado.
4. Clique em Salvar.

   A nova regra aparece na página Lista de regras de arquivamento e eliminação.

Mais informações:

Campos Regra de arquivamento e eliminação (na página 498)
Executar regras de arquivamento e eliminação (na página 495)

Campos Regra de arquivamento e eliminação

É possível usar os campos nas páginas Regra de arquivamento e eliminação para definir e editar as definições de regra.

Nome da regra

(Obrigatório) Especifica um identificador exclusivo da regra. Pode ser de até 30 caracteres alfanuméricos.

Status

(Obrigatório) Indica se essa regra está ativa ou inativa.

Cronograma

Especifica um turno de trabalho no qual a regra deve estar em vigor. Os turnos de trabalho são definidos pelo administrador.

Intervalo de repetição

Especifica com que frequência esta regra será executada, no formato horas:minutos:segundos (HH:MM:SS).

Nome do arquivo de arquivamento

Especifica o nome do arquivo em que você quer armazenar os registros desatualizados. Seu local é controlado pela variável NX_RULE_ARCHIVE_PATH armazenada no arquivo NX.env. Os arquivos de dados de arquivamento podem ser restaurados para o banco de dados com o utilitário PDM_LOAD.

Tipo de operação

Especifica um dos seguintes tipos de operações que a regra deve executar:

Arquivamento/Eliminação

Elimina do banco de dados registros antigos, que são gravados no arquivo especificado no campo Nome do arquivo de arquivamento.

Apenas eliminação

Elimina do banco de dados registros desatualizados, que não são gravados no arquivo de arquivamento.

Apenas arquivamento (execução de teste)

Grava registros desatualizados no arquivo de arquivamento sem eliminá-los do banco de dados. Use essa opção para testar uma regra de arquivamento e eliminação recém-criada ou editada.

Config. Nome do objeto

Especifica o nome do objeto de banco de dados que esta regra pode arquivar e eliminar.

Nome do objeto

(Somente leitura) Preenche a seleção no campo Config. o nome do objeto automaticamente.

Dias de inatividade

Especifica o número de dias que um registro fica inativo para se qualificar para o arquivamento e eliminação do banco de dados.

Consulta adicional

Arquiva e elimina registros inativos específicos entre os registros inativos existentes. Use este campo quando quiser criar regras diferentes para arquivamento e eliminação dos subconjuntos de registros expirados para o mesmo objeto. Use a mesma sintaxe usada para consultas armazenadas.

Exemplos: especificar consultas adicionais

A seguinte consulta arquiva e elimina apenas os registros de solicitação inativos atribuídos com uma prioridade de 1:

```
priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0
```

O formato de consulta a seguir arquiva e elimina registros com base no período:

```
close_date < EndAtTime(\'LAST_YEAR\')
```

Editar uma regra de arquivamento e eliminação

Você pode editar uma regra de arquivamento e eliminação que já foi criada.

Para editar uma regra de arquivamento e eliminação

1. Na guia Administração, selecione Regras de arquivamento e eliminação.

   A lista de regras de arquivamento e eliminação é exibida.

2. Selecione a regra que deseja editar e clique no nome da regra.

   A página de detalhes da Regra de arquivamento e eliminação é exibida.

3. Clique em Editar.

   A página Atualizar regra de arquivamento e eliminação é exibida.

4. Edite os campos conforme apropriado.

5. Clique em Salvar.

   Suas edições são salvas e a página Lista de regras de arquivamento e eliminação é exibida.

Mais informações:

Campos Regra de arquivamento e eliminação (na página 498)
Executar regras de arquivamento e eliminação (na página 495)

Histórico de arquivamento e eliminação

Você pode exibir um resumo das informações de histórico para cada regra de arquivamento e eliminação.

Para visualizar o histórico de arquivamento e eliminação

1. Selecione Arquivamento e eliminação, Histórico de arquivamento e eliminação na guia Administração.

   A página Lista de históricos de arquivamento e eliminação é exibida. Essa lista exibe uma entrada para cada vez que a regra foi executada.

2. Os seguintes campos são mostrados:

   Nome da regra

   Exibe o nome da regra usada na lista de histórico.

   hora de início

   Exibe a hora em que a regra foi iniciada.

   Hora de término

   Exibe a hora em que a regra foi concluída.

   Principais objetos eliminados

   Exibe os principais objetos que foram eliminados pela regra. Por exemplo, uma solicitação de chamada.

   Objetos filho eliminados

   Exibe os objetos filho relacionados que foram eliminados pela regra. Por exemplo, os logs de atividade de uma solicitação de chamada.

3. (Opcional) Clique em Mostrar filtro e especifique um critério de filtro para limitar a lista às informações que você quer.
4. Clique no nome de uma regra se você deseja revisar a configuração da regra.

   A página de detalhes da Regra de arquivamento e eliminação é exibida.

Filtrar Lista de históricos de arquivamento e eliminação

Você pode filtrar uma Lista de históricos de arquivamento e eliminação para exibir somente as entradas de interesse.

Para filtrar a Lista de históricos de arquivamento e eliminação

1. Selecione Mostrar filtro na página Lista de históricos de arquivamento e eliminação.

   A parte superior da página exibe os campos de filtro.

2. Complete os campos conforme o necessário para exibir as entradas que deseja ver:

   Nome da regra

   Selecione o nome da regra de arquivamento e eliminação cujo histórico deseja ver.

Primeira data de início

Insira a primeira data e hora para especificar o começo de um intervalo para filtrar o histórico para mostrar somente entradas para um intervalo de tempo especificado.

Última data de início

Insira a última data e hora para especificar o começo de um intervalo para filtrar o histórico para mostrar somente entradas para um intervalo de tempo especificado.

Primeira data de término

Insira a primeira data e hora para especificar o final de um intervalo para filtrar o histórico para mostrar somente entradas para um intervalo de tempo especificado.

Última data de término

Insira a última data e hora para especificar o final de um intervalo para filtrar o histórico para mostrar somente entradas para um intervalo de tempo especificado.

Observação: para exibir o campo Argumentos de pesquisa adicionais, clique no ícone spigot. Este campo é destinado apenas a usuários avançados que compreendem SQL e Majic e podem usá-lo para especificar argumentos de pesquisa que não estão disponíveis nos campos de filtro de pesquisa padrão. Para especificar um argumento de pesquisa adicional, digite uma cláusula SQL WHERE neste campo.

3. Clique em Pesquisar.

   A Lista de históricos de arquivamento e eliminação exibe as entradas que corresponde aos critérios de filtro.

Tratamento de anexos (arcpur)

Registros de anexos são salvos no banco de dados e arquivos de anexos são salvos no diretório do repositório. Ao arquivar e eliminar registros de anexos no banco de dados, eles são marcados como excluídos, mas não podem ser removidos. Esses registros são necessários para o daemon do repositório localizar os anexos.

Configurar o tipo de arquivamento

Você pode configurar o Tipo de arquivamento para anexos em um repositório a partir da guia Administração.

Para configurar o tipo de arquivamento

1. Navegue até a Biblioteca de anexos, Repositórios.

   A página Repositórios aparece.

2. Clique com o botão direito do mouse em um repositório (como Service Desk), selecione Exibir.

   A página Detalhes de Repositório aparece.

3. Clique em Editar.

   Selecione um dos seguintes da lista suspensa Tipo de arquivo morto:

   Nenhuma

   Nenhum processo de arquivamento e eliminação é realizado.

   Arquivamento e eliminação

   Os registros desatualizados são gravados no arquivo especificado no campo Nome do arquivo de arquivamento e eliminados do banco de dados.

   Apenas eliminação

   Os registros desatualizados são eliminados do banco de dados, mas não são gravados no arquivo de arquivamento.

4. Clique em Salvar.

   A página Detalhes de Repositório aparece, exibindo suas mudanças.

Observação: você não pode usar arquivamento e eliminação com Gerenciamento de conhecimento. Esse recurso tem suporte somente no CA SDM.

Configurar o caminho de arquivamento

Você pode configurar o caminho de arquivamento para anexos em um repositório a partir da guia Administração.

Para configurar o caminho de arquivamento

1. Navegue até a Biblioteca de anexos, Repositórios.

   A página Repositórios aparece.

2. Clique com o botão direito do mouse em um repositório (como Service Desk), selecione Exibir.

   A página Detalhes de Repositório aparece.

3. Clique em Editar.

   Insira o caminho no campo Caminho de arquivamento.

   O seguinte é o diretório padrão:

   $NX_ROOT/site/attachments/default/archived_files

4. Clique em Salvar.

   A página Detalhes de Repositório aparece, exibindo suas mudanças.

Como restaurar dados arquivados

Ao restaurar dados arquivados, você deve iniciar os daemons no modo dbadmin com o utilitário pdm_d_mgr. O modo dbadmin permite acesso limitado, portanto, é possível executar pdm_load com segurança para restaurar dados arquivados.

A seguir se encontra a descrição de como dados arquivados são restaurados:

1. Encerre o CA SDM.

2. Inicie os daemons no modo dbadmin, usando o seguinte comando:

   ```
   pdm_d_mgr -s DBADMIN
   ```

3. Localize o arquivo de dados arquivados. Por padrão, o arquivo está localizado em $NX_ROOT/site/data/archive.

4. Execute pdm_load no arquivo de dados. Por exemplo:

   ```
   pdm_load -a -f 2004611T1726_Call_Request.dat
   ```

5. Se houver um problema com o carregamento, verifique a linha de comando e o log quanto a erros. Arquivos Arcpur.log podem ser encontrados em $NX_ROOT/log.

   Observação: o limite de tamanho de arquivos arcpur.log está definido em $NX_ROOT/NX.env como:

   ```
   # The size limit for the Archive and Purge log file and data file.
   @NX_ARCPUR_FILESIZE=2000000000
   ```

   O arquivamento e eliminação criam arcpur.log.0, arcpur.log.1 até arcpur.log.9 após atingir o limite de arquivo para cada arquivo de log.

6. Execute pdm_halt.

   Isso encerra os daemons.

7. Reinicialize o CA SDM.

   Observação: após restaurar o registro, ele é arquivado e eliminado no próximo ciclo do processo de arquivamento e eliminação.

8. (Opcional) Para evitar que o arquivo seja arquivado e eliminado no próximo ciclo, faça o seguinte:

   a. Atualize o registro para torná-lo ativo novamente.

   b. Desative o arquivo e elimine a regra.

Arquivar e eliminar dados do KPI

As regras de Arquivamento e Eliminação predefinidas estão disponíveis para arquivar e eliminar dados do KPI. Navegue até Arquivamento e eliminação, Regras de Arquivamento e eliminação na guia Administração. Em seguida, filtre a lista, pesquisando regras inativas. É possível selecionar uma das seguintes regras e defini-la para Ativo:

- KPI_Data(SQL)
- KPI_Data(Stored Query)
- KPI_Data(System)
- KPI_Ticket_Data

Uma regra de configuração opcional pode ser criada dentro dos arquivos arcpur_cfg.xml e itil_arcpur_cfg.xml para arquivar e eliminar a tabela KPI_Ticket_Data.

É possível encontrar os arquivos nos seguintes diretórios:

- arcpur_cfg.xml

  $NX_ROOT\site\cfg\

- itil_arcpur_cfg.xml

  $NX_ROOT\site\cfg

Use os métodos a seguir para arquivar e eliminar a tabela KPI_Ticket_Data:

Tabela KPI_Ticket_Data

- Use end_time (last_mod_dt) em KPI_Ticket_data para determinar se um registro precisa ser arquivado e eliminado.

- Vincule os registros na tabela KPI_Ticket_Data aos registros na tabela Ticket (como cr, chg, ou iss). Isso garante que todos os registros relacionados a ticket na tabela KPI_Ticket_Data são arquivados e eliminados.

A tabela KPI_Ticket_Data não possui um relacionamento SREL com nenhuma tabela Ticket e conta com dois campos, obj_name, e obj_id, para vincular-se a um ticket. O valor obj_name pode ser cr, chg, ou iss e o valor obj_id é a id do ticket. Defina um main_obj para cada objeto de ticket.

A seguir há uma amostra de definição de main_object para o objeto de ticket, cr:

```
<!-- KPI Ticket Data -->
<main_obj>
<name>KPI Ticket Data</name>
<internal_name>KPI Ticket Data</internal_name>
<factory>ktd</factory>
<default_query>obj_name='cr'</default_query>
<date_field>end_time</date_field>
<ref_by value="obj_id">cr.id</ref_by>
</main_obj>
```

Observação: a regra de configuração pode selecionar apenas registros para cr. A marca ref_by pode corresponder o valor de obj_id nos dados de ticket do KPI para o valor da id em cr. Se uma correspondência for encontrada, isso significa que um registro de dados de ticket do KPI é mencionado por um registro cr, de modo que o registro de dados de ticket do KPI não seja arquivado ou eliminado.

Após adicionar as regras de configuração para todos os objetos de ticket, reinicie o serviço do CA SDM. Essas regras de configuração tornam-se nomes de objeto de configuração selecionáveis no formulário de detalhes de Regra de Arquivamento e Eliminação.

Fóruns do Gerenciamento de conhecimento sobre arquivamento e eliminação

Você pode usar as regras de arquivamento e eliminação para remover fóruns excluídos do banco de dados. Você pode criar uma regra de arquivamento e eliminação para arquivar e eliminar somente documentos do tipo Fórum.

Observação: se você não criar uma regra de arquivamento e eliminação, a regra de Documento de Conhecimento existente poderá arquivar e eliminar todos os documentos excluídos, incluindo os documentos do tipo Fórum.

Para criar uma regra para arquivamento e eliminação de fóruns

1. Navegue até Arquivamento e eliminação, Regras de Arquivamento e eliminação na guia Administração.

   A lista de regras de arquivamento e eliminação é exibida.

2. Clique em Criar novo.

   A página Criar Nova regra de arquivamento e eliminação aparece.

3. Faça o seguinte:

   - Selecione "documento de conhecimento" em Config. Lista suspensa Nome do objeto.
   - Adicione "KS_TYPE=20" ao campo Consulta adicional.

4. Clique em Salvar.

   A nova regra de arquivamento e eliminação é criada.

Capítulo 12: Usando a API de texto

Esta seção contém os seguintes tópicos:

API de texto (na página 509)
O arquivo de configuração (na página 524)

API de texto

API de texto é uma interface que permite usar entradas com base em texto para criar e atualizar objetos no banco de dados do CA SDM, como ocorrências, solicitações, contatos e ativos. Usando a API de texto, é possível atribuir valores à maioria dos campos que estão acessíveis aos usuários.

Importante: O CA SDM requer que todas as entradas sejam em formato UTF-8, ou os dados podem tornar-se corrompidos. O utilitário pdm_unconv (na página 1193) permite converter dados de um conjunto de caracteres locais em UTF-8, e de UTF-8 em um conjunto de caracteres locais.

Você pode acessar a API de texto usando as seguintes interfaces:

- Linha de comando
- Email
- CA NSM

Observação: é possível usar os serviços web como uma alternativa à API de texto para integração entre aplicativos.

Mais informações:

Métodos de conversão (na página 522)

Interface de linha de comando

Use o comando *pdm_text_cmd* para ativar a interface de linha de comando da API de texto. É possível então especificar certas informações, como a tabela a ser processada e a operação a ser executada, usando parâmetros do comando pdm_text_cmd.

A entrada da API de texto é passada ao comando pdm_text_cmd na forma de um arquivo de entrada ou diretamente do STDIN.

Observação: ao transmitir os parâmetros a partir do prompt de comando, use Ctrl+Z no Windows e Ctrl+D com o POSIX.

Importante: Você não pode usar aspas simples ou duplas como parâmetros para os comandos bop_cmd e pdm_text_nxd.

Mais informações:

pdm_text_cmd--Interface da linha de comando API do texto (na página 1190)

Interface do CA Network and Systems Management

Quando o CA NSM e o CA SDM estão integrados e você cria solicitações a partir de eventos do CA NSM, o parâmetro user_parms nas definições de regra de elaborador é passado à API de texto. O processo de elaborador do CA SDM (tngwriter) define seus próprios parâmetros de substituição para alterar o texto antes de enviá-lo à API de texto. A palavra-chave LOG_AGENT é adicionada ao final da entrada para definir o log_agent para a solicitação.

Observação: é necessário atualizar o arquivo Text_API.cfg para todos os campos adicionais que são passados dos Sistemas de gerenciamento de alertas do CA NSM para o CA SDM. Este arquivo é usado para integrações com serviços web, email e AHD.DLL.

Mais informações:

Palavras-chave (na página 512)

Formato de entrada

A entrada para a API de texto é especifica das seguintes formas:

- Na interface de linha de comando, a entrada é tipicamente especificada em um arquivo de texto passado para o comando pdm_text_cmd.
- Na interface de email, a entrada é especificada no texto do email. Você especifica uma expressão comum para localizar os identificadores do objeto de destino.

Você formata a entrada da API de texto da mesma forma, não importa a interface que usar.

O formato básico da entrada é o seguinte:

```
%palavra-chave=valor
```

ou

PROPERTY={{rótulo_propriedade**}}**valor

O comportamento normal dos comandos da API de texto tem as seguintes exceções, onde a última ocorrência de dois ou mais comandos conflitantes tem precedência:

- Quando uma mensagem contém vários objetos ID de ticket válidos que correspondem à sequência de caracteres de filtro da caixa de correio, ou vários comandos da ID de ticket da API de texto, o primeiro encontrado é usado. Além disso, um objeto ID de ticket, que é identificado usando a sequência de caracteres de filtro de caixa de correio, sobrescreve qualquer comando da ID de ticket da API de texto, independentemente de qual aparecer primeiro.
- Quando uma mensagem contém vários comandos da API de texto de comentário de log, todos os comentários são publicados, apesar de que a ordem em que aparecem no log de atividade do ticket pode variar.

Todos os objetos ID de ticket que correspondem ao filtro, válidos ou não, e os comandos da ID de ticket da API de texto dentro da mensagem, aplicáveis ou não, são comentados antes que a mensagem seja publicada. Os objetos ID de ticket identificados por meio de filtros de regra de caixa de correio aparecem como -((...))-. Sinais de porcentagem à esquerda (%) em comandos da ID de ticket da API de texto são convertidos em dois parênteses de abertura ((, e dois parênteses de fechamento)) seguem-se ao comando. Se o comando da ID de ticket da API de texto aparecer depois de outro comando da API de texto com um comentário de log (%LOG=...), então o comando comentado da ID de ticket da API de texto é feito em um comentário de log separado.

Observação: o comentário de log é o único comando da API de texto que pode aparecer várias vezes em uma mensagem e ainda assim ter cada ocorrência aplicada. Para qualquer outro comando, a API de texto usa somente a última ocorrência, porque várias ocorrências de outros comandos conflitam entre si. Vários comandos de comentário de log publicam mensagens de comentário de log separadas para o ticket, e não necessariamente em qualquer ordem particular.

Adicionalmente, se um comando da ID de ticket da API de texto aparecer na mensagem, seja no início da mensagem ou entre dois outros comandos da API de texto, ele é convertido em um comentário de log. Se o comando anterior é um comentário de log (%LOG=...) ou descrição de atualização (%DESCRIPTION=...), ele é anexado a aquele comando, em vez de tornar-se um comentário de log separado.

Mensagens de entrada que são enviadas somente como HTML, sem uma versão em texto sem formatação incluída, perdem seu corpo de mensagem. Se a mensagem coincidir com qualquer filtro de regra de caixa de correio com um corpo de mensagem vazio, um ticket pode ser criado com uma Descrição vazia, ou com o assunto da mensagem como toda a descrição do ticket.

Palavras-chave

Você pode usar dois tipos de palavras-chave como entrada para a API de texto.

- As definições na seção [KEYWORDS] do arquivo text_api.cfg - este tipo é um grupo de palavras-chave relacionadas diretamente aos campos das várias tabelas que você pode atualizar. Por exemplo, a maioria dos campos no formulário Issue Detail é definida na seção [KEYWORDS]. Ao usar essas palavras-chave, você pode definir valores para campos no registro que atualizar ou criar. Por exemplo, a seguinte linha define a prioridade da ocorrência como 5:

  ```
  %PRIORITY=5
  ```

  A seção [KEYWORDS] do arquivo text_api.cfg lista todas as palavras-chave. É possível definir palavras-chave adicionais (por exemplo, para permitir acesso da API de texto a campos que foram adicionados durante a personalização do esquema de banco de dados).

- As palavras-chave especiais a seguir são sempre definidas como abaixo, independentemente do conteúdo do arquivo text_api.cfg:

Palavra-chave	Descrição
ASSET	Usado para anexar um item a um ticket (válido para solicitações, ocorrências e requisições de mudança). O valor especificado é o nome do item, o qual já deve existir. É possível especificar essa palavra-chave várias vezes, pois um ticket pode ter vários itens anexados a ele.
ATTACHMENT	Usada internamente pela interface de email para adicionar anexos de email a um ticket.
DESCRIÇÃO	Especifica o valor a usar para o campo de descrição do ticket. Essa palavra-chave é adotada quando a entrada é enviada à API de texto sem uma palavra-chave explícita. Esta palavra-chave é aplicada automaticamente pelo Mail Eater quando a mensagem não inicia com a palavra-chave, mas contém um artefato ou palavra-chave da ID de ticket. Você pode alterar o modo como a palavra-chave DESCRIPTION é tratada para atualizações usando a seguinte entrada na seção [OPTIONS] de text_api.cfg: UPDATE_DESC_IS_LOG Se essa opção for definida como YES (SIM), o valor será usado para criar um comentário de log. Se o valor for definido como NO (NÃO), o valor substitui o campo existente de descrição.
FROM_EMAIL FROM_EMAIL_OVERRIDE	Usados pela interface de email para fazer a correspondência com o campo de Endereço de email no registro de ca_contact. Também é usado como o log_agent para o ticket. Se ambos forem fornecidos, FROM_EMAIL é ignorado. **Observação:** FROM_EMAIL é definido automaticamente pelo Mail Eater com o endereço do remetente da mensagem.
FROM_PERSID	Usado pela interface de linha de comando para definir o log_agent para uma operação (por exemplo, quando um registro de ca_contact não possui uma ID de usuário). Esta palavra-chave é passada automaticamente por pdm_text_cmd se o -parâmetro p for especificado. O valor é combinado com a persistent_id do registro ca_contact.

Palavra-chave	Descrição
FROM_USERID	Usado apenas na interface de linha de comando para definir o log_agent para uma operação. Esta palavra-chave é passada automaticamente por pdm_text_cmd se o -parâmetro u for especificado. O valor é combinado com a ID de usuário de um contato.
LOG	Usado para criar uma entrada de log (válido para solicitações, requisições de mudança, ocorrências e contatos). Esta palavra-chave é aplicada automaticamente pelo Mail Eater quando a mensagem não inicia com uma palavra-chave, mas contém um artefato ou uma palavra-chave da ID de ticket, ou a palavra-chave DESCRIPTION.
LOG_AGENT	Usado pela interface do CA NSM para definir o log_agent de uma operação. O valor é analisado em relação ao campo ID do registro de um contato.
PROPERTY	Usado para definir o valor de uma propriedade (válido apenas para solicitações, requisições de mudança e ocorrências). Diferentemente de outras palavras-chave, que são seguidas por um sinal de igual e um valor, a sintaxe da palavra-chave PROPERTY deve incluir o rótulo de propriedade, como mostrado a seguir: PROPERTY={{rótulo_propriedade}}valor Você deve especificar o *rótulo_propriedade* exatamente como aparece no banco de dados.
SEARCH	Usada apenas na interface de linha de comando e na interface do CA NSM para fornecer uma lista de palavras-chave para uso em uma consulta para atualizar vários tickets de um ativo. O valor é uma lista de palavras-chave usadas na pesquisa. A palavra-chave SEARCH é definida automaticamente pela interface do CA NSM.
SEARCH_EXPLICIT	Usada apenas na interface do CA NSM para substituir a palavra-chave SEARCH fornecida pela interface do CA NSM. Os valores fornecidos são os mesmos que os usados com a palavra-chave SEARCH.

Mais informações:

pdm_text_cmd--Interface da linha de comando API do texto (na página 1190)

Convenções de entrada de palavra-chave

As seguintes convenções aplicam-se à formatação de entrada de palavra-chave:

- Todas as palavras-chave (incluindo PROPERTY) devem ter um sinal de por cento (%) como prefixo. O sinal de por centro deve estar na posição um da coluna. Se a primeira linha não vazia da entrada não tiver um sinal de por cento no início, %DESCRIPTION= ou %LOG= é usado como prefixo para os dados recebidos, dependendo de se uma palavra-chave ou um objeto da ID de ticket foi encontrado. Se for definido %DESCRIPTION, os conteúdos da mensagem até a primeira palavra-chave são postados como uma descrição de ticket. Se for definido %LOG, os conteúdos da mensagem até a primeira palavra-chave são postados como um comentário de log.
- Não use espaços entre o sinal de porcentagem e a palavra-chave, nem entre a palavra-chave e o sinal de igual (=).
- Não inclua valores entre aspas; todos os dados depois do sinal de igual são considerados como o valor.
- Palavras-chave não diferenciam maiúsculas de minúsculas.
- Se a entrada incluir palavras-chave duplicadas, a última palavra-chave é usada; caso contrário, a ordem em que você especificou os pares palavra-chave/valor não é importante.
- Especifique valores de palavra-chave como faria para o campo correspondente na interface da Web. Por exemplo, para especificar um tipo de contato Analista, você usaria %CONTACT_TYPE=Analyst, embora no banco de dados esse valor esteja armazenado como um número inteiro. A palavra-chave CONTACT_TYPE é definida em text_api.cfg, de modo que o valor especificado é convertido (na página 522) para corresponder ao valor armazenado.

  Observação: se o valor diferencia entre maiúsculas e minúsculas dependente do DBMS subjacente.
- Você pode distribuir os dados de seqüências de caracteres em várias linhas.

Formatar uma mensagem de email para atualizar um ticket

Um usuário pode formatar uma mensagem de email para criar ou atualizar um ticket.

Para formatar uma mensagem de email para criar ou atualizar um ticket, use os seguintes campos:

Para

Especifica o nome da caixa de correio atribuído ao contato do CA SDM configurado para o usuário privilegiado.

De

Especifica a pessoa enviando o email. A pessoa deve ser definida na tabela ca_contact, a menos que a opção Permitir anônimo esteja especificada na regra da caixa de correio aplicável.

Observação: o endereço De normalmente é parte da configuração do programa de email, e normalmente não é configurado em uma base por mensagem.

Anexos

Anexa documentos e outros arquivos ao email para enviar anexos à API de texto.

Assunto

Combina palavras-chave em uma sequência de caracteres de filtro de regras da caixa de correio, particularmente ao criar um ticket.

Corpo

Especifique o corpo da mensagem do email usando a API de texto. Você pode especificar a palavra-chave ISSUE_ID, REQUEST_ID ou CHANGE_ID, dependendo do tipo de ticket para criar ou atualizar um ticket.

Delimitadores de início e final de mensagens de email

Algumas interfaces de email adicionam informações ao começo ou ao final de mensagens de email (por exemplo, codificação MIME) isso pode fazer com que a interface de email não funcione corretamente. Se a sua interface de email adiciona informações, é possível usar os seguintes delimitadores: start-request e end-request. A interface de email ignora as informações especificadas antes de start-request e depois de end-request.

Observação: o Mail Eater não oferece suporte a emails nos formatos RTF ou somente HTML.

Exemplo: use delimitadores start-request e end-request

```
"start-request"
message_body
"end-request"
```

Como a API de texto usa objetos

A API de texto processa o assunto ou corpo de notificações de email. Regras da caixa de correio permitem identificar objetos e valores que a API de texto usa. Por exemplo, é possível definir a regra para incidentes como Incident:{{object_id}}, então encontrar Incident:1234 se traduz para %INCIDENT_ID=1234 para a API de texto. 1234 é o ref_num para o Incidente. Porque o objeto deve ser único em um email e fácil de encontrar, você pode tornar o objeto mais distinto, como %Incident:{{object_id}}%.

Siga a palavra-chave {{object_id}} do objeto com um caractere que não seja uma letra, número, vírgula, barra (/), sinal de mais (+) ou sinal de igual (=), porque esses caracteres podem aparecer em um objeto. Caso contrário, é possível que os caracteres que seguem o objeto sejam mal interpretados como parte do valor do objeto, ou que um caractere no valor do objeto seja mal interpretado como o caractere que segue o valor.

O Mail Eater faz o seguinte:

1. Encontra o objeto em um email (como Incidente:1234) que mapeia para o ticket adequado ou outro objeto suportado pela API de texto.
2. Traduz o objeto em um token de API de texto (como %INCIDENT_ID=1234).

3. O Mail Eater envia a mensagem de destino para a API de texto. A API de texto processa o email, aplica o texto, comandos ou ambos que contém ao ticket adequado e gera um email de resposta automática indicando se a mensagem de email recebida foi aplicada com sucesso. Dependendo das ações realizadas, uma mensagem de email de notificação também é enviada separadamente para indicar certos eventos específicos, como a criação de um ticket.

Como configurar respostas de notificação para atualizar tickets

O daemon da API de texto (pdm_text_nxd) cria e atualiza tickets com informações de interfaces externas, como linha de comando e email. É possível configurar o correio para usar a API de texto de modo que os usuários (contatos) possam atualizar tickets respondendo notificações de email. O texto da resposta é adicionado como uma atividade de comentário de log para o ticket.

Para configurar respostas de notificação para atualizar tickets, faça o seguinte:

1. Defina o método de notificação que o contato usa para pdm_mail –T *reply_email_address* ou pdm_mail –F *reply_email_address.* O *reply_email_address* especifica o endereço de chegada para a caixa de correio. Quando o contato clica em responder em um email, esse endereço é preenchido a partir do endereço De ou Responder a da mensagem à qual está respondendo.

   -T define o endereço Responder para. -F define o endereço De, usado como o endereço de resposta se um endereço separado não for especificado.

   Observação: alguns programas de correio não honram ou não podem honrar um endereço Responder para.

2. Criar ou atualizar uma regra da caixa de correio usando uma palavra-chave da API de texto.

   Os objetos definidos pelo usuário nos filtros de regra da caixa de correio substituem as seguintes palavras-chave da API de texto:

Objeto	Palavra-chave da API de texto	Identificador
Incidente	%INCIDENT_ID	Ref_num
Problema	%PROBLEM_ID	Ref_num
Solicitação	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num

Objeto	Palavra-chave da API de texto	Identificador
Ocorrência	%ISSUE_ID	Ref_num

3. Criar ou atualizar uma frase de notificação que corresponde à regra.
4. Criar ou atualizar um modelo de mensagem que use a frase notificação.
5. Atualizar a regra da caixa de correio criada na Etapa 2 para especificar o modelo de mensagem que você criou ou atualizou na Etapa 4.

Observação: para obter informações sobre a realização de cada etapa, consulte a *Ajuda online*.

Após o usuário receber a notificação e respondê-la, as seguintes ações ocorrem:

1. Quando a sequência de caracteres de filtro é encontrada a palavra-chave da ID de ticket relevante e o valor denotado pelo espaço reservado, se houver, são anexados à mensagem.
2. Se um objeto da ID de ticket correspondente for encontrado, o ticket correspondente é atualizado com um comentário de log, uma nova descrição ou outros valores, de acordo com o texto, palavras-chave e comandos na mensagem.
3. Se um objeto da ID de ticket correspondente não for encontrado, é criado um ticket com uma descrição e outros parâmetros de acordo com o texto, palavras-chave e comandos na mensagem.

Exemplo de como configurar uma resposta a uma notificação de incidente

Este exemplo mostra como configurar uma resposta a uma notificação de incidente

Para configurar uma resposta a uma notificação de incidente, faça o seguinte:

1. Crie uma regra da caixa de correio usando os seguintes campos e valores:
   - Filtro—Corpo contém
   - Sequência de caracteres de filtro—%Incident:{{object_id}}%
   - Ignorar maiúsculas e minúsculas—SIM
   - Ação—Atualizar objeto
   - Objeto de ação—Incidente

2. Criar uma frase de notificação que inclua a regra como segue:
   - Símbolo—Resposta a incidente
   - Código—IncidentReply
   - Ativo—Ativo
   - Descrição—Comentário que integra a resposta para um Incidente/problema/solicitação.
   - Frase—para adicionar um comentário a @{call_req_id.type.sym}, apenas responda este email ou inclua a linha abaixo (em uma linha própria).

     ```
     %Incident:{call_req_id.ref_num}%
     ```

     Observação: no texto de resposta automática da regra da caixa de correio, omita o prefixo call_req_id. . Esse prefixo aplica um contexto no qual o texto da regra da caixa de correio já está, e tal mudança de contexto não é válida quando já estiver atuando nesse contexto.
3. Criar ou atualizar um modelo de mensagem que use a frase notificação como segue:
   - Corpo da mensagem de notificação

     ```
     Esta é uma notificação simples.
     @{notification_phrase[IncidentURL1].phrase}
     ```
4. Atualizar a regra da caixa de correio criada na Etapa 1 para especificar o modelo de mensagem criado na Etapa 3, como segue:

   Modelo de mensagem—*nome da regra da caixa de correio*

Como um usuário final atualiza um exemplo de ticket

O seguinte exemplo demonstra como um usuário final (John Smith) responde a uma notificação de email para atualizar um ticket de incidente.

O Corpo ou Assunto do email inclui o identificador de objeto. O local reservado {{object_id}} na sequência de caracteres do filtro denota o identificador de objeto.

1. Uma notificação é enviada para John Smith e inclui as seguintes instruções:
   ```
   Para adicionar um comentário ao seu incidente, basta responder a este email ou
   incluir a linha abaixo (em uma linha própria).
   %Incident:1234%
   ```
2. John Smith responde a notificação como segue:
   ```
   Esta é minha resposta...
   ```

3. O Mail Eater recebe a seguinte versão de texto do email de John Smith:

```
Esta é minha resposta...

De: Service Desk
Enviado: quarta-feira, 18 de Setembro de 2009 10h22
Para: Smith, John
Assunto: Notificação Simples

Esta é uma notificação simples.

Para adicionar um comentário ao seu incidente, basta responder a este email ou
incluir a linha abaixo (em uma linha própria).

%Incident:1234%
```

4. O Mail Eater processa regras em ordem e encontra o objeto %Incident:1234%:

```
Esta é minha resposta...

De: Service Desk
Enviado: quarta-feira, 18 de Setembro de 2009 10h22
Para: Smith, John
Assunto: Notificação Simples

Esta é uma notificação simples.

Para adicionar um comentário ao seu incidente, basta responder a este email ou
incluir a linha abaixo (em uma linha própria).
%INCIDENT_ID=1234
```

5. O Mail Eater adiciona as palavras-chave da API de texto e o valor {{object_id}} para a instrução %INCIDENT_ID= e deixa um marcador onde o valor {{object_id}} foi encontrado. O seguinte texto mostra os dados que são enviados para a API de texto. O texto em negrito mostra valores adicionados pelo Mail Eater.

```
%LOG=Esta é a minha resposta...
De: Service Desk
Enviado: quarta-feira, 18 de Setembro de 2009 10h22
Para: Smith, John
Assunto: Notificação Simples

Esta é uma notificação simples.

Para adicionar um comentário ao seu incidente, basta responder a este email ou
incluir a linha abaixo (em uma linha própria).
%Incident:-((...))-%
%FROM_EMAIL=john.smith@company.com
%INCIDENT_ID=1234
```

6. A API de texto adiciona um comentário de log para o Incidente 1234.

Métodos de conversão

Muitas das palavras-chave definida em text_api.cfg têm um método associado para converter o valor especificado a um valor que seja apropriado para armazenamento no banco de dados. Esse recurso permite que os usuários especifiquem valores do mesmo modo que fariam na interface da web, sem ter nenhum conhecimento da implementação subjacente.

O arquivo de configuração possui diversos exemplos desse tipo de definição de palavras-chave, incluindo ISSUE.PRIORITY e CONTACT.CONTACT_TYPE. Caso precise definir palavras-chave adicionais (por exemplo, para permitir que a API de texto acesse campos adicionados ao personalizar o esquema do banco de dados), é possível usar um dos seguintes métodos predefinidos:

Método	Tipo de saída
lookup_actbool	INTEIRO
lookup_asset_by_name	UUID
lookup_asset_by_persid	UUID
lookup_chg_category	SEQÜÊNCIA
lookup_chg_status	SEQÜÊNCIA
lookup_cnt_by_email	UUID
lookup_cnt_by_last_first_middle	UUID
lookup_cnt_by_logonid	UUID
lookup_cnt_by_persid	UUID
lookup_cnt_meth	INTEIRO
lookup_cnt_type	INTEIRO
lookup_company	UUID
lookup_cr_status	SEQÜÊNCIA
lookup_cr_template	SEQÜÊNCIA
lookup_domain	INTEIRO
lookup_grc	INTEIRO
lookup_group	UUID
lookup_impact	INTEIRO

Método	Tipo de saída
lookup_iss_category	SEQÜÊNCIA
lookup_iss_status	SEQÜÊNCIA
lookup_loc	UUID
lookup_mfr_model	UUID
lookup_nr_family	INTEIRO
lookup_org	UUID
lookup_person_contacting	INTEIRO
lookup_position	INTEIRO
lookup_priority	INTEIRO
lookup_prob_category	SEQÜÊNCIA
lookup_product	INTEIRO
lookup_resource_status	INTEIRO
lookup_service_lvl	SEQÜÊNCIA
lookup_severity	INTEIRO
lookup_state	INTEIRO
lookup_timezone	SEQÜÊNCIA
lookup_type_of_contact	INTEIRO
lookup_urgency	INTEIRO
lookup_workshift	SEQÜÊNCIA

Se o valor que você necessita converter não puder utilizar um desses métodos predefinidos, será necessário escrever um método personalizado. O método deve tomar como entrada um valor de SEQÜÊNCIA e retornar um valor (NÚMERO INTEIRO, SEQÜÊNCIA ou UUID) como sua saída. Retorne um valor -1 (ou "-1") para indicar que o valor não pode ser determinado e, portanto, não foi definido. No caso de UUID, retorne um "(uuid) NULL".

Por exemplo, é possível desenvolver um método para converter uma ID de usuário em uma referência da tabela ca_contact. O valor de entrada, como Administrador, seria passado ao método, o qual retornaria a ID da tabela ca_contact para a ID de usuário do Administrador.

A maneira em que você define palavras-chave no arquivo de configuração oferece a vantagem de definir vários mapeamentos de palavra-chave ao mesmo campo, incluindo métodos diferentes de conversão, de acordo com o valor sendo especificado. Por exemplo, o destinatário pode ter vários mapeamentos diferentes de palavra-chave para definir como configurar seu valor com base em valores de entrada diferentes. Uma entrada pode ser uma ID de usuário, outra pode ser o sobrenome, nome, segundo nome, e outra ainda pode conter a ID real de ca_contact (por exemplo, 793ED69B4E87A545BD8E911834D829FC). Todas as palavras-chave apontam a métodos de conversão diferentes, exceto a última, que não necessita ser convertida.

O arquivo de configuração

O arquivo text_api.cfg define as palavras-chave diretamente relacionadas aos campos das várias tabelas que você pode atualizar. Esse arquivo pode ser usado como uma fonte de referência para localizar certos valores predefinidos, como palavras-chave, e como um mecanismo para configurar a API de texto, embora o arquivo de configuração padrão funcione para a maioria das instalações sem modificações.

O arquivo text_api.cfg está localizado no seguinte diretório:

- UNIX—$NX_ROOT/site
- Windows—*diretório de instalação*\site. Por exemplo: C:\Arquivos de programas\CA\Service Desk\site

O arquivo de configuração é dividido em seções, com atributos particulares definidos em cada seção. As definições de atributo estão no seguinte formato:

```
palavra-chave=valor
```

Nenhuma das palavras-chave diferencia maiúsculas de minúsculas, porém todos os valores (exceto aquelas na seção [OPTIONS]) diferenciam maiúsculas de minúsculas.

Observação: é possível visualizar e modificar o arquivo text_api.cfg usando qualquer editor de texto.

Importante: Se você está fazendo integração com o componente Alert Management Systems do CA NSM, é necessário atualizar o text_api.cfg para quaisquer campos adicionais que sejam passados para o CA SDM.

Mais informações:

Palavras-chave (na página 512)

Opções

A seção [OPTIONS] do arquivo text_api.cfg define opções de processamento que podem diferir de um site para outro. Por exemplo, há opções para determinar o formato de entrada de data, que campos permitem a retenção de alimentação de linha e se ocorrências, solicitações e requisições de mudança pode ou não ser atualizadas usando a interface de email. Todas as opções nesta seção podem ser configuradas. Saiba que, embora possa remover nomes de tabela da VALID_TABLE_LIST, se você não quiser dar à API de texto o acesso a essas tabelas, não adicione nomes de tabela a essa lista.

Padrões

Use a seção [XX_DEFAULTS] fornecida no arquivo text_api.cfg para cada interface usando a API de texto (por exemplo, [EMAIL_DEFAULTS] para a interface de email e [CMD_DEFAULTS] para a interface da linha de comando). A seção [XX_DEFAULTS] define os valores padrão para campos e propriedades que são exigidos caso o usuário não os forneça diretamente. XX se refere ao tipo de interface, como CMD ou EMAIL.

Para definir valores padrão, use um dos seguintes formatos:

- nome_tabela**.**palavra-chave**=**valor

  A *palavra-chave* deve ser definida na seção [KEYWORDS] ou como propriedades em seu banco de dados. Qualquer método associado à palavra-chave é automaticamente aplicado ao *valor.* Por exemplo:

  ```
  ISSUE.PRIORITY=1
  ```

  A palavra-chave PRIORITY é definida em text_api.cfg para executar uma pesquisa para converter o valor especificado por você a fim de corresponder ao valor similar armazenado no banco de dados. Aqui, o valor 1 é convertido em 5, que é o valor do banco de dados subjacente do símbolo de prioridade 1. Esse recurso permite que os usuários especifiquem o valor do mesmo modo como fariam na interface web.

- nome_tabela.**PROPERTY={{r**ótulo_propriedade**}}**valor

  O *rótulo_propriedade* deve ser definido como uma propriedade em seu banco de dados.

Em ambos os formatos, o *nome_tabela* deve ser um dos valores definidos por VALID_TABLE_LIST na seção [OPTIONS],como Ocorrência, Solicitação ou Contato.

Mais informações:

Métodos de conversão (na página 522)

Ignorar entrada

Há várias seções [..._IGNORE_INCOMING] no arquivo text_api.cfg, uma para cada interface que usa a API de texto (por exemplo, [TNG_IGNORE_INCOMING] para a interface CA NSM e [EXT_IGNORE_INCOMING] para a interface externa usado por outros produtos CA). Essas seções definem campos e propriedades que são ignorados na entrada (o formato é o mesmo que o descrito em Padrões, porém nenhum "**=***valor*" é especificado). Esse recurso permite evitar que os usuários configurem certos valores, o que, por sua vez, fornece mais segurança para aquelas vezes em que os clientes usam a interface de email.

As seções IGNORE funcionam bem quando usadas em conjunto com as seções [..._DEFAULTS] correspondentes, pois é possível impedir que o usuário defina um determinado valor e forneça um valor padrão ao mesmo tempo. Por exemplo, se quiser impedir que usuários de interface de email definam a prioridade de uma ocorrência, você poderá definir os seguintes valores:

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

Nesse caso, qualquer prioridade que o usuário especifique no corpo da mensagem de email será ignorada, e todas as ocorrências criadas pela interface de email terão uma prioridade 2 automaticamente atribuídas.

Entrada de exemplo

Os exemplos a seguir mostram as entradas que você pode usar no corpo de uma mensagem de email ou em um arquivo que funcione como entrada para a interface de linha de comando.

Exemplo: a primeira linha não inclui uma palavra-chave

Neste exemplo, como falta uma %palavra-chave na primeira linha da primeira coluna, o valor literal %DESCRIPTION= é adicionado ao começo da mensagem. Isso define o campo de descrição como "Esse texto inteiro será incluído no campo de descrição" (com a quebra de linha intacta, pois a entrada ISSUE.DESCRIPTION está incluída na lista de campos da entrada LINEFEEDS_ALLOWED na seção [OPTIONS] de text_api.cfg).

```
Esse texto inteiro será incluído
no campo de descrição
%PRIORITY=None
```

Exemplo: a primeira linha inclui uma palavra-chave

Neste exemplo, a palavra-chave PRIORITY é definida em text_api.cfg para executar uma procura para converter o valor especificado por você em um valor correspondente armazenado no banco de dados. Aqui, o valor None é convertido em 0, que é o valor do banco de dados subjacente do símbolo de prioridade 1. Esse recurso permite aos usuários especificar valores do mesmo modo como fariam na interface da web.

```
%description=Esta é minha descrição
%priority=Nenhum
%CATEGORY=Upgrade.PC
%PROPERTY={{CPU Atual}}266 mhz
%PROPERTY={{Disco Rígido Atual}}1 gig
%PROPERTY={{Atualização Solicitada}}disco rígido de 4 gig
```

Os valores especificados são usados para definir a descrição e os campos de prioridade do ticket, de modo semelhante ao exemplo anterior (observe que a palavra-chave pode estar em minúsculas ou maiúsculas).

O valor de Upgrade.PC é pesquisado, e o campo de categoria do ticket é definido de modo apropriado.

Fazer a correspondência entre os rótulos a seguir define os três valores de propriedade:

- CPU Atual
- Disco Rígido Atual
- Atualização Solicitada

Capítulo 13: Gerenciando controle de versão

Observação: Neste capítulo, a maior parte das referências a “cliente” aplica-se tanto a um cliente como a um servidor secundário.

Esta seção contém os seguintes tópicos:

Como funciona o controle de versão (na página 529)
Arquivos de controle de versão (na página 530)
Arquivos de controle do servidor primário (na página 530)
Arquivos de controle do servidor secundário e cliente (na página 531)
Controle de versão para personalizações de instalação (na página 532)
Modos de servidor de controle de versão (na página 533)
Sintaxe do arquivo de controle de versão (na página 534)

Como funciona o controle de versão

O controle de versão do CA SDM ajuda a administrar personalizações do sistema que afetam clientes e servidores secundários. Você pode usar o controle de versão em instalações cliente e servidor secundário.

O controle de versão funciona da seguinte maneira:

1. Quando um cliente se conecta ao servidor, o cliente envia uma lista de seus componentes controlados ao servidor.
2. O servidor compara a lista a sua própria lista mestra.
3. Se o servidor encontrar alguma diferença, você pode fazer o seguinte:
   - Notifique o cliente.
   - Cancele a tentativa de conexão.
   - Atualize o cliente para a versão correta dos componentes controlados.

Observação: o controle de versão não é um sistema de distribuição de software; o recurso de atualização simplesmente fornece um modo de corrigir pequenos problemas de sincronização entre cliente e servidor.

Arquivos de controle de versão

O CA SDM mantém dois conjuntos de arquivos de controle de versão. Um conjunto é para servidores secundários e o outro, para todos os clientes. Um componente controlado pode representar um arquivo, um diretório ou o arquivo de variável de ambiente client_nx.env. Um componente também pode ser genérico; isto é, não estar associado a qualquer objeto externo. É possível usar um componente genérico para fornecer controle de versão para o cliente como um todo ou para um arquivo ou diretório grande demais para uma atualização automática. A falta de correspondência entre componentes de versão genéricos não resulta em uma atualização automática. A falta de correspondência sempre resulta em uma falha do cliente e deve ser corrigida manualmente.

Arquivos de controle do servidor primário

O controle de versão no servidor do CA SDM consiste de um executável, pdm_ver_nxd, e dois arquivos de controle de versão, server_default.ver e server_secondary.ver. A opção de servidor ver_ctl determina como o controle de versão responde a discrepâncias de versão entre componentes instalados no servidor e no cliente. A configuração padrão da opção ver_ctl do Gerenciador de opções é UPGRADE, fazendo com que o controle de versão seja atualizado quando uma discrepância é detectada.

O Pdm_ver_nxd valida mensagens de solicitação de versão de clientes ao comparar os dados na solicitação com os seguintes arquivos de controle de versão:

- server_default.ver
- server_secondary.ver
- server_custom.ver
- server_secondary_custom.ver

Se pdm_ver_nxd detecta uma discrepância entre versões de componentes, ele registra uma mensagem sobre o problema e, como ATUALIZAR está habilitado, o cliente é atualizado. O conteúdo da mensagem de notificação depende das configurações da opção ver_ctl.

Se desejar, é possível criar e manter os dois arquivos *personalizados* de controle de versão abaixo para gerenciar personalizações:

- server_secondary_custom.ver
- server_custom.ver

Arquivos de controle do servidor secundário e cliente

O controle de versão em um servidor secundário ou cliente do CA SDM consiste em um executável (pdm_ver) e um arquivo de controle de versão (secondary.ver). Se desejar, é possível criar e manter um segundo arquivo de controle de versão para administrar personalizações: server_secondary_custom.ver.

O software cliente inclui um executável, pdm_ver, e um arquivo de versão padrão, default.ver. O controle de versão criará automaticamente um segundo arquivo de versão (custom.ver) no cliente se um arquivo server_custom.ver existir no servidor. Os dois arquivos de versão de cliente controlam as versões de componentes padrão e personalizados instalados no cliente.

A configuração padrão da opção ver_ctl do Gerenciador de opções é UPGRADE, fazendo com que o controle de versão atualize o servidor secundário quando uma discrepância é detectada. A verificação de versão é executada apenas em servidores secundários e clientes remotos (não há a necessidade de controlar a versão em clientes executados no servidor primário, porque o servidor contém as cópias mestras de todos os componentes). O controle de versão é sempre executado no servidor primário. Quando um servidor secundário ou cliente é iniciado, ele lê seus arquivos de versão e envia uma mensagem ao servidor primário listando todos os componentes instalados e suas versões. Se uma discrepância entre versões de componentes ocorrer, o servidor determina sua resposta verificando a configuração da opção ver_ctl. A resposta do servidor informa ao cliente se ele deve continuar, terminar ou atualizar componentes.

Observação: a maioria dos clientes recebe o download de arquivos e variáveis de opção durante sua inicialização. Isso reflete as opções escolhidas pelo administrador quando o servidor foi configurado e as opções instaladas.

Controle de versão para personalizações de instalação

Se você personalizar seu cliente do CA SDM, poderá usar o controle de versão para monitorar e controlar a instalação das personalizações nos clientes. Para fazê-lo, crie um arquivo server_custom.ver (ou server_secondary_custom.ver para servidores secundários) descrevendo suas personalizações.

O controle de versão usa os dois arquivos de versão (server_default.ver e server_custom.ver) de forma independente para verificar a versão de componentes nos clientes. Seus componentes devem ser projetados de modo que um arquivo nunca seja controlado por dois ou mais componentes. O controle de versão processa cada componente separadamente. O controle de versão verifica um arquivo sempre que encontra um componente que controla o arquivo, o que às vezes tem resultados inesperados se o número da versão ou a data não forem iguais.

Para usar o controle de versão para monitorar e controlar a instalação de personalizações nos clientes, siga essas etapas:

1. Crie o arquivo server_custom.ver em um dos seguintes locais:
   - Linux — $NX_ROOT/site/mods/server_custom.ver
   - Windows — diretório de -instalação\site\mods\server_custom.ver
2. Adicione componentes ao server_custom.ver para cada uma de suas mudanças, usando uma das seguintes configurações:
   - Crie componentes dir_ctl para implementar o controle de versão no nível de diretório. Quando você faz essa configuração, todos os arquivos no diretório são considerados como da mesma versão e são atualizados ao mesmo tempo. Isso restringe a necessidade de manutenção a server_custom.ver, mas às vezes pode resultar na atualização de arquivos já atualizados no cliente.
   - Crie componentes file_ctl para implementar o controle de versão no nível de arquivo. Essa configuração fornece melhor documentação e controle, mas o arquivo server_custom.ver pode ser maior.
3. Atualize o número da versão em server_custom.ver sempre que fizer uma mudança em um componente personalizado. O número da versão permite ao controle de versão reconhecer clientes com versões diferentes.

Modos de servidor de controle de versão

A opção de servidor ver_ctl determina como o controle de versão responde a discrepâncias de versão entre componentes instalados no servidor e no cliente. Essa opção pode ser definida com o Gerenciador de opções.

A opção ver_ctl pode ter um dos seguintes valores:

NOTIFICAR

(Cliente Windows) Pergunta se o usuário quer continuar ou sair se uma discrepância de versão for detectada.

(Cliente Linux) Gera um log da discrepância de versão, mas o cliente sempre conclui a inicialização. Nenhum arquivo é alterado para corrigir a discrepância.

ANULAR

Encerra o cliente se uma discrepância de versão for detectada. O usuário não consegue usar o CA SDM até que o cliente seja manualmente atualizado.

DESABILITAR

Ignora discrepâncias de versão. Todos os clientes recebem autorização de conexão.

Observação: os clientes podem definir sua própria opção ver_ctl como DESABILITAR para ignorar o controle de versão.

ATUALIZAR

Pergunta se o cliente quer atualizar os componentes afetados para a versão correta se uma discrepância de versão for detectada. Se a atualização for bem-sucedida, a conexão do cliente continuará; caso contrário, a conexão do cliente será encerrada. O método de atualização depende do tipo de controle de versão do componente.

A seguir estão algumas configurações válidas:

Definição	Descrição
dir_ctl	O cliente adiciona, atualiza ou exclui arquivos no diretório usando cópias fornecidas pelo servidor. O diretório em si nunca é excluído.
file_ctl	O cliente adiciona, atualiza ou exclui o arquivo usando uma cópia fornecida pelo servidor.

Definição	Descrição
nxenv_ctl	O cliente atualiza seu arquivo NX.env.
ver_ctl	Um componente ver_ctl não pode ser atualizado. Uma discrepância neste tipo de componente faz com que a sessão do cliente seja terminada sem que ele se conecte ao servidor.

Sintaxe do arquivo de controle de versão

Cada arquivo de controle de versão descreve um ou mais componentes. Um componente pode representar um arquivo, diretório ou o arquivo de variável de ambiente client_nx.env. Um componente também pode ser genérico; isto é, não estar associado a qualquer objeto externo.

Observação: para obter mais informações sobre a estrutura e a sintaxe de arquivos de controle de versão, consulte os arquivos .ver que são instalados em seu sistema no subdiretório do local do diretório de instalação principal do CA SDM. Esses arquivos têm comentários úteis e configurações de exemplo que podem ser úteis.

Use a seguinte sintaxe para definir cada componente. Itens com letras em *itálico* representam dados fornecidos por você. O *nome_do_componente* e os parâmetros de versão são sempre exigidos. Outros parâmetros podem ser exigidos, dependendo do valor de *tipo de controle*. Todos os outros itens representam palavras-chave que você deve digitar exatamente como mostrado no exemplo a seguir:

```
[ nome do componente ]
version = "x.x, yyyymmdd"
tipo de controle
filename = "nome de arquivo"
directory = "diretório"
link = "diretório do link"
source = "diretório de origem"
effectivity = "especificação de efetividade"
checksum
min_release = "versão"
max_release = "versão"
component_type = "tipo de arquivo"
o_mode = "modo-proprietário"
g_mode = "modo-grupo"
w_mode = "mode-mundial"
```

Parâmetros de controle de versão

Os seguintes parâmetros se aplicam ao controle de versão:

[nome do componente]

Especifica o nome de um item sob controle de versão. O nome deve ser exclusivo e colocado entre colchetes. *O nome do componente* não diferencia maiúsculas de minúsculas. Esse parâmetro é obrigatório para iniciar uma definição componente.

version="x.x. yyymmd"

Especifica um número de versão (*x.x*) e uma data (*yyymmdd*) que definem a versão do componente. Esse parâmetro é exigido, e deve ser incluído com aspas duplas. O controle de versão verifica a versão de um componente ao comparar o número da versão e sua data no servidor com o número de versão e data no cliente. Tanto o número da versão como a data devem corresponder nos componentes para que sejam considerados sincronizados entre cliente e servidor. Opcionalmente, se a propriedade checksum estiver habilitada, o arquivo será verificado pela soma de verificação antes de ser atualizado.

tipo de controle

Especifica o tipo de controle de versão para esse componente. As configurações a seguir são válidas para o tipo de controle:

Definição	Descrição
dir_ctl	Especifica que o componente representa um diretório. Você deve fornecer o parâmetro de diretório para especificar o caminho ao diretório. Você também pode fornecer o parâmetro de nome de arquivo para especificar uma máscara para arquivos no diretório a serem atualizados quando uma atualização é exigida. Os subdiretórios não são atualizados no UNIX ou Windows.
file_ctl	Especifica que o componente representa um arquivo. Você deve fornecer o diretório e os parâmetros de nome de arquivo para especificar o caminho ao arquivo.
Nxenv_ctl	Especifica que esse componente representa o arquivo client_nx.env, que é usado para armazenar variáveis de ambiente internas do CA SDM. O controle de versão do CA SDM e o Gerenciador de opções mantêm este arquivo automaticamente. Há um componente nxenv_ctl, e seu nome de componente deve ser CLIENT_NXENV.

Definição	Descrição
ver_ctl	Esse é o tipo de controle padrão. Ele especifica que o componente é genérico; isto é, ele não está associado a qualquer objeto externo específico. É possível usar um componente genérico para fornecer controle de versão para o cliente como um todo ou para um arquivo ou diretório grande demais para uma atualização automática. Os componentes com um tipo de controle ver_ctl não podem ser atualizados; a falta de correspondência entre versões de um componente ver_ctl quando o servidor está em modo ATUALIZAR causa a falha da conexão do cliente.

filename="nome de arquivo"

Especifica o nome de um arquivo sob controle de versão. Não contém especificações de diretório. Esse parâmetro é exigido para componentes file_ctl, mas é opcional para componentes de controle de diretório (dir_ctl). Quando usado com componentes de diretório, o parâmetro de nome de arquivo age como uma máscara de arquivo para restringir os arquivos associados ao componente dir_ctl. Por exemplo, se o nome de arquivo de um componente dir_ctl for *.README, então uma atualização desse diretório incluirá apenas arquivos terminados em “.README.”.

directory="diretório"

Especifica o caminho do diretório dos componentes dir_ctl, ou do diretório contendo o arquivo para componentes file_ctl. Esse parâmetro é ignorado em componentes ver_ctl e nxenv_ctl. O caminho do diretório deve ser incluído entre aspas e pode conter referências a variáveis de ambiente precedidas por $.

Observação: sempre use barras normais (e não barras invertidas) para separar subdiretórios no nome de caminho, mesmo em um servidor Windows.

link="diretório de link"

Especifica um diretório de link no cliente no mesmo formato descrito previamente para o parâmetro de diretório. Esse parâmetro é opcional para componentes file_ctl e dir_ctl, e é ignorado em componentes ver_ctl e nxenv_ctl. Se for especificado, uma atualização a um cliente Linux pode fazer com que um link simbólico seja colocado no diretório de link, apontando para o arquivo real copiado ao local especificado pelo parâmetro de diretório. Uma atualização a um cliente Windows faz com que o arquivo real seja copiado aos locais do link e de diretório.

source="diretório de origem"

(Opcional) Especifica um diretório diferente no servidor onde o servidor pode recuperar arquivos a serem fornecidos. Esse parâmetro tem o mesmo formato descrito previamente para o parâmetro de diretório. Isto é útil se os arquivos que devem ser entregues ao cliente são diferentes dos mesmos arquivos que se encontram no local de diretório no servidor. Esse parâmetro é usado para instruir o servidor a recuperar o arquivo do *diretório de origem* e entregá-lo ao local no cliente especificado pelo parâmetro de diretório. O parâmetro de diretório é necessário quando você especifica o parâmetro de origem.

effectivity="especificação de efetividade"

(Opcional) Especifica se o cliente deve receber esse componente. Permite excluir alguns clientes do download. Se um cliente não for incluído na especificação de efetividade, ele não receberá o componente. Se este parâmetro for omitido, todos os clientes receberão o componente. A especificação de efetividade usa os seguintes símbolos:

+ (sinal de adição)

Indica a adição de um grupo de cliente.

- (sinal de subtração)

Indica a exclusão de um grupo de cliente.

Os seguintes grupos de clientes são válidos:

- SUN4SOL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS
- UNIX_CLIENTS

Por exemplo, a seguinte especificação indica que apenas os clientes UNIX devem receber os arquivos:

```
effectivity = "+ UNIX_CLIENTS"
```

checksum

Determina a atualização do componente se a soma de verificação do componente no cliente não corresponder à soma de verificação no servidor. Quando aplicado a um diretório, a soma de verificação é aplicada a cada arquivo.

min_release="release" e max_release="release"

Especifica o cliente mais antigo e o mais recente aos quais esse componente deve ser distribuído. As declarações no arquivo server_default.ver definem as versões. Esses parâmetros estão no seguinte formato, onde Ga*xx* indica a versão e os valores subseqüentes são genlevels associados à versão.

```
! Release GA50 50MVV000900 50W7T000900
! Release GA45 45MW000900 50WTT000900
```

A requisição indica que GA50 é mais recente do que GA45.

[nome do componente]

Especifica o nome de um item sob controle de versão. O nome deve ser exclusivo e colocado entre colchetes. *O nome do componente* não diferencia maiúsculas de minúsculas. Esse parâmetro é obrigatório para iniciar uma definição componente.

Definição	Descrição
arquivo	Esse é o tipo de componente padrão. Especifica que os arquivos copiados ao cliente devem ser obtidos diretamente do local no servidor indicado pelo parâmetro de diretório.

Definição	Descrição
exe_file	Especifica que os arquivos copiados ao cliente devem ser obtidos de um local no servidor que depende do sistema operacional do cliente, como mostrado a seguir: ■ windows (Windows) ■ sun4Sol (Solaris) ■ hp (HP-UX) ■ (aix—AIX) ■ linux (Linux) ■ linux390 (Linux390) Os locais para esses subdiretórios dependem do configuração de parâmetro de diretório. Se esse parâmetro estiver definido, os subdiretórios estarão localizados sob o *diretório* indicado. Do contrário, estarão localizados sob o diretório bin do diretório de instalação principal do CA SDM.

o_mode="modo-proprietário"

Especifica permissões de acesso de arquivo para o proprietário do arquivo.

g_mode="modo-grupo"

Especifica permissões de acesso de arquivo para usuários no grupo do proprietário do arquivo (usados apenas com clientes UNIX).

w_mode="mode-mundial"

Especifica permissões de acesso de arquivo para usuários que não fazem parte do grupo do proprietário do arquivo (usados apenas com clientes UNIX).

Os três parâmetros de modo permitem que versões diferentes do mesmo executável sejam mantidas no servidor. Eles especificam controles de acesso ao arquivo quando ele é copiado ao cliente. Esses parâmetros são usados apenas durante uma operação de atualização. Eles consistem de um a três caracteres, que significam o seguinte:

Definição	Descrição
S	Read (Leitura)
W	Write (Gravação)
v	Execute

Os clientes de PC ignoram as permissões de Gravação e Execução.

Você pode especificar qualquer combinação de um ou mais modos de acesso de arquivo. Em clientes UNIX, o arquivo apresenta o modo de acesso especificado. Em clientes de PC, o arquivo é gravável ou somente leitura, dependendo da especificação de w_mode.

Remover o controle de um componente

Você talvez tenha de remover o controle de um componente, porém se você simplesmente excluir o componente do arquivo server_default.ver do servidor primário, os arquivos associados também serão excluídos. Em vez disso, você pode definir um bloco *uncontrol* no arquivo server_default.ver, o que permite excluir o componente sem excluir os arquivos associados nos clientes. Essas declarações têm o seguinte formato:

```
! uncontrol component-name
```

Essa declaração indica que esse componente não é mais controlado. Os clientes que se conectam a esse servidor devem remover esse componente de seu arquivo de versão, e também devem remover os arquivos associados a esse componente. Você pode remover o bloco uncontrol depois que os clientes tiverem se conectado com êxito ao menos uma vez.

Observação: é necessário atualizar todos os clientes usando o cliente com o controle de versão mais recente. Os clientes com controle de versão mais antigo podem ignorar componentes sem controle.

Capítulo 14: Gerenciamento de itens de configuração

Esta seção contém os seguintes tópicos:

Usando a interface da Web (na página 541)
ICs Contato, Local e Organização (na página 546)
Relacionamentos do CI (na página 550)
Versão (na página 559)
Exibir atributos de IC em outros produtos CA (na página 589)
Usando o visualizador do CMDBf (na página 590)
CMDB Visualizer (na página 590)
Adicionar um ativo detectado (na página 594)
Sinalizadores Ativo e IC (na página 595)
CI Reconciliation (na página 597)
Gerenciar Transações armazenadas temporariamente (na página 620)
Manutenção de dados do CA CMDB (na página 647)
CACF (Configuration Audit and Control Facility) (na página 663)

Usando a interface da Web

Dependendo da sua função, é possível realizar tarefas de usuário e de administração em ICs (configuration items - itens de configuração) usando os seguintes recursos:

- Gerenciadores de filas permitem realizar tarefas de usuário e gerenciar ICs e relacionamentos de ICs.
- A guia Administração permite realizar tarefas de administração com ICs e relacionamentos..
- O CMDB Visualizer permite realizar tarefas de usuário e de administração para visualizar ICs e relacionamentos.

Mais informações:

Exibir itens de configuração (na página 542)
Criar um item de configuração (na página 543)
Atualizar um item de configuração (na página 543)
Associar uma janela de manutenção a um IC (na página 544)
Exibir janelas de mudança associadas (na página 545)
Exibir o histórico do item de configuração (na página 545)
Desativar um item de configuração (na página 545)
Reativar um item de configuração (na página 546)

Exibir itens de configuração

O Placar permite abrir um item de configuração e exibir informações sobre ele.

Para abrir e exibir um item de configuração

1. A partir do Gerenciador de filas, clique em Pesquisar, Itens de configuração.

   É exibido o painel Pesquisa de item de configuração.

2. Digite os critérios de pesquisa e clique em Pesquisar.

   A Lista de itens de configuração é exibida e relaciona os resultados da pesquisa.

3. (Opcional) Clique em um item de configuração na coluna Nome para abri-lo e exibir suas informações detalhadas.

   Os detalhes do item de configuração são exibidos.

Observação: após criar um IC, a página Detalhes do IC não exibe alguns atributos de identificação se estiverem em branco (não tiverem um valor) e não se aplicarem à família do IC. Entretanto, sempre é exibida a identificação de atributos com valores não em branco.

Criar um item de configuração

O Placar permite criar um item de configuração.

Para criar um item de configuração

1. A partir de Gerenciador de filas, clique em Arquivo, Novo item de configuração.

   A página Criar item de configuração aparece.

2. Digite um nome exclusivo para o item de configuração no campo Nome.
3. Digite a classe do item de configuração no campo Classe ou clique no ícone de pesquisa acima do campo para localizar uma classe.
4. Preencha todos os campos restantes aplicáveis ao novo item de configuração.

   Observação: apenas Nome e Classe são valores obrigatórios para a criação de um item de configuração.

5. Clique em Continuar.

   A página Criar novo item de configuração exibe guias e campos adicionais.

6. Digite os dados necessários nos campos adequados na guia Atributos.

   Os atributos que aparecem na guia são determinados pela família da classe selecionada para o item de configuração. As informações inseridas aqui são determinadas pelos processos de negócio e pelas informações que você deseja armazenar e exibir para um item de configuração.

7. Clique em Salvar.

   É exibida uma mensagem que confirma a criação do item de configuração.

Atualizar um item de configuração

O Placar permite modificar um item de configuração.

Para modificar um item de configuração

1. Em Gerenciador de filas, localize e abra o item de configuração.

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Para alterar as informações do item de configuração, selecione as guias apropriadas na página e insira os novos dados nos campos. Clique em Salvar.

   É exibida uma mensagem que confirma a modificação do item de configuração.

Observação: sempre que um IC for atualizado usando a opção –a, a data e o usuário da última mudança do IC exibidos na Lista de itens de configuração são atualizados, mesmo se nenhum atributo foi alterado. Essa atualização ocorre se um IC foi editado na interface de usuário (e salvo sem mudanças) ou atualizado usando o GRLoader.

Associar uma janela de manutenção a um IC

Para controlar o acesso de manutenção a um IC, é possível associar esse IC a uma ou mais janelas de manutenção não globais.

Para associar uma janela de manutenção a um IC

1. Navegue para a página Detalhes do IC.
2. Clique na guia Janelas de manutenção.

   A Lista de janelas de manutenção aparece.
3. Clique em Atualizar janelas de manutenção.

   A página Pesquisas de janelas de manutenção aparece.
4. Especifique informações para as janelas de manutenção necessária.
5. Clique em Pesquisar.

   As Janelas disponíveis são exibidas.
6. Mova quaisquer janelas obrigatórias na lista Janelas de mudança disponíveis para a lista Janelas de mudança associadas.
7. Clique em OK.

   As associações de nova janela, janelas de mudança e ICs são salvos.

Exibir janelas de mudança associadas

Para determinar como um IC pode ser afetado durante períodos de tempo específicos, é possível exibir as janelas de manutenção associadas a esse IC.

Para exibir janelas de mudança associadas a um IC

1. Navegue para a página Detalhes do IC.
2. Clique na guia Janelas de manutenção.

   As janelas de manutenção associadas são exibidas.

Exibir o histórico do item de configuração

Você pode exibir o histórico de um item de configuração.

Para exibir o histórico de um item de configuração

1. Pesquise e abra o item de configuração.

   A página Detalhe de item de configuração aparece.
2. Clique na guia Versão.

   A página Controle de versão é exibida.
3. Clique em Mostrar log.

   O histórico do item de configuração é relacionado.

   Observação: a opção Mostrar log ignora as seleções no painel esquerdo.

Desativar um item de configuração

Se um item de configuração não for mais usado, é possível editar os detalhes do item de configuração para desativá-lo. O status inativo retira o item de configuração da Lista de itens de configuração do Gerenciador de filas. Não é possível excluir um item de configuração.

Observação: desativar uma família ou classe não afeta os ICs existentes na família e na classe em questão. Essa ação apenas impede que novos ICs sejam criados nessa família ou classe.

Para desativar um item de configuração

1. Pesquise e abra o item de configuração.

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Selecione Inativo na lista suspensa Ativo. Clique em Salvar.

   Aparece uma mensagem que confirma a mudança de status. O item de configuração não aparece mais na lista de itens de configuração ativos. O item de configuração continua a aparecer em todos os relacionamentos existentes até que estes sejam desativados.

Reativar um item de configuração

Se for necessário usar um item de configuração inativo, é possível reativá-lo.

Para reativar um item de configuração

1. Pesquise e abra o item de configuração.

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Selecione Ativo na lista suspensa Ativo. Clique em Salvar.

   Aparece uma mensagem que confirma a mudança de status. O item de configuração aparece na lista de itens de configuração ativos.

ICs Contato, Local e Organização

Uma instalação do CA CMDB pode definir ICs para *objetos base*: Contatos, Locais e Organizações. Esses ICs podem ser gerenciados adequadamente e estabelecer relacionamentos com outros ICs, conforme desejado. Para alguns clientes, essa abordagem oferece melhor suporte ao processo de gerenciamento de configuração do que empregar objetos base apenas como atributos de ICs.

Mais informações:

Criar um IC a partir de um objeto básico (na página 547)
Selecionar um objeto base para um IC (na página 548)
Editar detalhes do IC de um objeto base (na página 548)
Editar atributos do IC de um objeto base (na página 549)
Criar IC de um objeto base usando o GRLoader (na página 550)

Criar um IC a partir de um objeto básico

O Placar permite criar um item de configuração a partir de um objeto base.

Para criar um IC a partir de um objeto base

1. Clique em Arquivo, Novo item de configuração.

   A página Criar item de configuração aparece.

2. Preencha os campos do IC. Nome e a Classe são obrigatórios. Clique em Continuar.

   Observação: os atributos comuns de IC (Nome do host, Número de série, Endereço Mac e Nome DNS) não são relevantes para um IC de um objeto base.

   A página Criar item de configuração aparece.

3. Clique no link do objeto base para definir o objeto que esse IC representa.
4. Selecione o objeto. É possível pesquisar um objeto existente ou clicar em Criar novo para criar um objeto. Se você deseja criar um objeto, clique em Salvar para continuar.

   O objeto selecionado aparece na parte superior da página Detalhes do item de configuração.

5. Clique em Salvar.

   Os principais atributos do objeto selecionado aparecem na guia Atributos da página Detalhes do item de configuração.

Selecionar um objeto base para um IC

É possível selecionar um objeto base para um item de configuração.

Para selecionar um objeto base para um IC

1. Selecione um IC na família do objeto base (Contato, Local ou Organização).

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Na seção superior, preencha os campos necessários para o objeto base. É possível digitar um valor diretamente ou clicar na lupa para pesquisar o objeto. Por exemplo, para pesquisar um contato, preencha um ou mais campos de pesquisa na janela Pesquisa de contato e clique em Pesquisar. Em seguida, selecione um contato na lista exibida.

4. Clique em Salvar.

   Se o objeto selecionado já estiver representado por um IC diferente na mesma família, uma mensagem de erro será exibida. Selecione um objeto diferente para modificar o IC.

Editar detalhes do IC de um objeto base

Você pode editar atributos do objeto básico que o IC representa, como ID de IC alt e Observações, da mesma maneira que em qualquer outra janela Detalhes do item de configuração.

Para editar os atributos do objeto base representado pelo IC

1. Selecione um IC na família do objeto base.

   A página Detalhe de item de configuração aparece.

2. Clique no link do objeto na parte superior da página.

   A página Detalhes do objeto é exibida.

3. Clique em Editar.

   A página Atualizar do objeto é exibida.

4. Edite os campos conforme desejado e clique em Salvar.

   A página Atualizar é fechada.

   Caso você tenha modificado um dos atributos exibidos na guia Atributos da página Detalhes do item de configuração, a mudança é exibida nela após a atualização da página.

Editar atributos do IC de um objeto base

É possível editar os atributos do item de configuração de um objeto base.

Para editar os atributos de um IC

1. Selecione um IC na família do objeto (Contato, Local ou Organização).

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Na guia Atributos, clique em Editar.

   A página Atualizar aparece.

4. Edite os campos conforme desejado e clique em Salvar.

   A página Atualizar é fechada.

5. Clique em Salvar.

   A página Detalhes do item de configuração exibe o IC modificado.

Criar IC de um objeto base usando o GRLoader

É possível usar o GRLoader para criar um IC de objeto de base a partir de um objeto de base existente.

Para usar o GRLoader para criar um IC de objeto de base a partir de um objeto de base existente

1. Grave o XML que identifica o seguinte:
   - Nome do CI
   - Família
   - Classe
2. Enviar o XML.

   O objeto de base é criado e o GRLoader exibe que um IC foi lido e inserido.

Exemplo: criar um IC a partir de um contato existente

O exemplo a seguir cria um IC a partir do contato existente **Gibbs, Keith**.

```
<GRLoader>
<ci>
    <name>Gibbs, Keith</name>
    <family>Contato</family>
    <class>Técnica</class>
    <base_contact>Gibbs, Keith</base_contact>
</ci>
</GRLoader>
```

Relacionamentos do CI

A funcionalidade do CA SDM depende dos relacionamentos entre itens de configuração. Relacionamentos de IC possuem as seguintes características:

- O *tipo de relacionamento* define como dois itens de configuração estão relacionados.
- Tipos de relacionamentos hierárquicos são combinados como *provedor/dependente*. Por exemplo, A (provedor) *hospeda* B; B (dependente) *é hospedado por* A.
- Tipos de relacionamento não hierárquicos são definidos como *ponto a ponto*. Por exemplo, *está conectado a*, que é o mesmo em qualquer direção.

Você pode fazer as seguintes funções de relacionamento usando a guia Relacionamentos do CMDB:

- Exibir relacionamentos Ativos ou Inativos pesquisando em Ativo? campo.
- A partir da Lista de relacionamentos de ICs, é possível clicar em qualquer link para um relacionamento para executar a página CI Relationship Detail.

Mais informações:

Tipos de relacionamentos de ICs (na página 551)
Criar um tipo de relacionamento (na página 552)
Gerenciar um relacionamento de IC (na página 553)
Criar um relacionamento de IC (na página 553)
Exibir relacionamentos de um IC (na página 554)
Desativar um relacionamento de IC (na página 554)
Reativar um relacionamento de IC (na página 555)
Desativar Relacionamentos do IC (Editar na lista) (na página 555)
Desativar um relacionamento de IC usando o GRLoader (na página 556)
Reativar um relacionamento de IC usando o GRLoader (na página 557)
Excluir um relacionamento de IC do banco de dados (na página 558)
Comparação e histórico de relacionamento do IC (na página 559)

Tipos de relacionamentos de ICs

O CA SDM fornece uma lista de tipos predefinidos de relacionamentos que podem ser usados para descrever um relacionamento ou associação entre itens de configuração. O modo em que o relacionamento é expresso depende de qual item de configuração em foco. Por exemplo, um provedor *oferece suporte* a um item de configuração dependente, mas o dependente *é suportado pelo* provedor. Há diferentes expressões do mesmo relacionamento, e o rótulo de tipo de relacionamento que você vê depende de como você está visualizando um relacionamento, de provedor para dependente ou de dependente para provedor.

Observação: para obter informações sobre os tipos de relacionamento fornecidos pelo CA CMDB, consulte o Guia de Referência Técnica do *CA CMDB*.

Criar um tipo de relacionamento

É possível criar um tipo de relacionamento e torná-lo disponível para criar ou atualizar relacionamentos.

Para criar um tipo de relacionamento

1. Na guia Administração, expanda a pasta do CA CMDB na seção esquerda.
2. Clique em Tipos de relacionamentos de ICs

   A Lista de tipos de relacionamento de ICs aparece na seção direita.
3. Clique em Criar novo.

   A página Criar novo tipo de relacionamento de ICs aparece.
4. Preencha os seguintes campos:

   Rótulo Provedor para dependente

   Descreve o relacionamento de provedor para o dependente, e é o nome que aparece na lista de tipos de relacionamento. Por exemplo, "atende" ou "gerencia" é um relacionamento de Provedor para dependente.

   Rótulo Dependente para provedor

   Descreve o relacionamento de dependente para provedor, e é o nome que aparece na lista de tipos de relacionamento. Por exemplo, "tem como prestador de serviços" ou "é gerenciado por" é um relacionamento Dependente para Provedor.

   Ponto a ponto?

   Especifica que o relacionamento não possui um IC provedor e um IC dependente, mas consiste em dois ICs iguais. Por exemplo, "conecta-se a" e "tolera falhas" são relacionamentos ponto a ponto.

   Ativo?

   Disponibiliza o tipo de relacionamento para seleção nos relacionamentos de item de configuração e para aparece na lista.
5. Clique em Salvar.

   O tipo de relacionamento é criado e você pode usá-lo para criar ou atualizar relacionamentos.

Gerenciar um relacionamento de IC

A página Relacionamento de itens de configuração fornece todas as configurações necessárias em um local para simplificar o processo de relacionamento do IC.

Você pode usar a página para realizar as seguintes funções:

- Alterar o relacionamento fornecedor/dependente entre dois ICs.

  Clique em Reverter para alternar o IC fornecedor e o IC dependente para o relacionamento. O IC focal muda. Se o relacionamento revertido não for válido, clicar em Reverter limpa o campo Relacionamento.

- Configurar campos Ótimos como Símbolo, Descrição e Custo.

  Clique em Opcional para definir campos opcionais.

  Se um Símbolo não for fornecido, é gerado automaticamente um Símbolo exclusivo com o prefixo **cmdb bmhier:**, além de um número exclusivo quando o relacionamento é criado.

  Observação: Se sua instalação for integrada com o CA Network and Systems Management (CA NSM), você é solicitado a especificar o repositório e custo do CA NSM.

Criar um relacionamento de IC

É possível adicionar um relacionamento de ICs a partir de um item de configuração focal.

Para adicionar um relacionamento a partir de um IC focal

1. Selecione o IC ao qual deseja adicionar um relacionamento.

   A página Detalhes do CI aparece.

2. Clique em Editar.

   A página Atualizar CI aparece.

3. Clique na guia Relacionamentos do CMDB e clique em Criar novo.

   A página Criar relacionamento de ICs aparece.

4. Especifique o IC Provedor. É possível clicar no link de lupa para pesquisar o IC.

   Observação: dependendo do relacionamento que deseja, é possível clicar em Reverter para alternar entre as posições de provedor/dependente.

5. Especificar um tipo de relacionamento É possível clicar no link da lupa para pesquisar o tipo de relacionamento.

6. Especifique o outro IC (por padrão, o IC dependente). É possível clicar na lupa para pesquisar o IC.

7. Clique em Salvar.

   O relacionamento é criado.

Exibir relacionamentos de um IC

Você pode exibir relacionamentos para um IC.

Para exibir relacionamentos de um IC

1. Navegue para o item de configuração.

   A página Detalhe de item de configuração aparece.

2. Selecione a guia Relacionamentos do CMDB.

   É exibida uma lista de relacionamentos do IC.

Desativar um relacionamento de IC

É possível desativar o relacionamento de IC, definindo seu status em Inativo.

Para desativar um relacionamento

1. Navegue até a página Detalhes do IC, clique na guia Relacionamentos do CMDB e em Editar.

   A guia Relacionamentos do CMDB é exibida no modo Edição.

2. Escolha um relacionamento e clique em qualquer link em sua linha.

   A página Detalhes do relacionamento de IC é exibida.

3. Clique em Editar.

4. Defina o atributo Ativo? como Inativo. Clique em Salvar.

   O relacionamento se torna Inativo. Na página Detalhes do relacionamento, o atributo “Ativo?” exibe o valor do atributo Inativo.

Reativar um relacionamento de IC

Você pode reativar um relacionamento de IC excluído.

Para reativar um relacionamento de IC excluído

1. Navegue para a página Detalhes do IC.

   A página Detalhes do IC é exibida em modo somente leitura.

2. Clique em Editar.

   A página Detalhes do IC é exibida no modo de edição.

3. Clique na guia Relacionamentos do CMDB.
4. Clique em qualquer link em uma linha para abrir a página de Detalhes do relacionamento do IC.
5. Clique em Editar.

   A página Atualizar relacionamento do IC aparece.

6. Altere o atributo Ativo? para “Ativo”. Clique em Salvar.

   O relacionamento é reativado.

Desativar Relacionamentos do IC (Editar na lista)

É possível Desativar um ou mais relacionamentos do IC usando o recurso Editar na lista.

Para desativar um ou mais relacionamentos do IC

1. Na guia Administração, abra a pasta do CA CMDB na seção esquerda.

   O nó do CA CMDB expande-se para exibir as subpastas.

2. Clique na pasta Lista de relacionamentos do CI.
3. (Opcional) Especificar filtros de pesquisa
4. Clique em Pesquisar.

   Os relacionamentos de ICs são exibidos no painel direito.

   Observação: por padrão, todos os relacionamentos são exibidos.

5. Clique em Editar na lista no canto superior direito da lista.

   Os controles de Editar na lista de Relacionamento são exibidos.

6. Selecione a linha que contém o relacionamento que deseja modificar.

   As exibições e os controles da linha são preenchidos com os valores do relacionamento.

7. Defina o atributo Ativo? como Inativo.

   Clique em Salvar se deseja Desativar somente o relacionamento destacado ou clique em Alterar tudo se deseja Desativar todos os relacionamentos ma pesquisa filtrada.

Desativar um relacionamento de IC usando o GRLoader

É possível Desativar um relacionamento do IC usando o GRLoader para enviar XML.

Para Desativar um relacionamento usando o GRLoader

1. Grave o XML que usa a marca Relação para identificar o seguinte:
   - IC do provedor
   - IC dependente
   - Tipo de relacionamento
2. Defina delete_flag como verdadeira (ou sim ou 1).
3. Enviar o XML.

   O Relacionamento do IC é excluído.

Observação: para obter mais informações sobre o GRLoader, consulte o *Guia de Referência Técnica do CA CMDB*.

Exemplo: excluir um relacionamento do IC usando o GRLoader

No exemplo a seguir de XML, o relacionamento 'estabelece conexão com' entre ci_1 e ci_2 é excluído.

```
<GRLoader>
        <relation>
                <dependent>
                        <name>ci_2</name>
                </dependent>
        <type>estabelece conexão com </type>
                <provider>
                        <name>ci_1</name>
                </provider>
        <delete_flag>true</delete_flag>
        </relation>
</GRLoader>
```

Reativar um relacionamento de IC usando o GRLoader

É possível reativar um relacionamento do IC usando o GRLoader para enviar XML.

Para reativar um relacionamento do IC usando o GRLoader

1. Grave o XML que usa a marca Relação para identificar o seguinte:
    - Tipo de relacionamento
    - IC dependente
    - IC do provedor
2. Defina delete_flag como falso (ou não ou 0).
3. Enviar o XML.

    O Relacionamento do IC é reativado.

Observação: para obter mais informações sobre o GRLoader, consulte o *Guia de Referência Técnica do CA CMDB*.

Exemplo: reativar um relacionamento do IC

No exemplo a seguir de XML, o relacionamento "estabelece conexão com" entre ci_1 e ci_2 é reativado.

```
<GRLoader>
        <relation>
                <dependent>
                        <name>ci_2</name>
                </dependent>
        <type>estabelece conexão com </type>
                <provider>
                        <name>ci_1</name>
                </provider>
        <delete_flag>false</delete_flag>
        </relation>
</GRLoader>
```

Excluir um relacionamento de IC do banco de dados

Você pode excluir um relacionamento de IC de modo que não esteja apenas Desativado, mas removido do banco de dados permanentemente.

Para remover um relacionamento do banco de dados

1. Navegue até Lista de relacionamentos do IC.

   A lista Relacionamentos do CI é exibida:

2. Clique com o botão direito do mouse em qualquer linha de relacionamento e selecione Excluir.

   O relacionamento é removido do banco de dados.

Importante: se o relacionamento excluído possuir um Símbolo definido, qualquer relacionamento com o mesmo Símbolo também será removido do banco de dados.

Comparação e histórico de relacionamento do IC

A guia Controle de versão exibe relacionamentos de IC e permite fazer o seguinte:

- Visualizar o histórico de relacionamento para qualquer IC no CMDB. As mudanças feitas em um relacionamento são registradas automaticamente quando o relacionamento é criado, atualizado ou excluído. É possível visualizar todos os relacionamentos atuais e históricos para um IC.

  Observação: os relacionamentos criados em versões anteriores do CA CMDB não possuem informações de histórico de auditoria.

- Comparar relacionamentos em qualquer instantâneo ou marco.

Versão

O controle de versão proporciona controle sobre a infraestrutura de TI acompanhando e gerenciando os ciclos de vida de todos os ICs que constituem o estado autorizado do CMDB. O controle de versão também se aplica à auditoria do histórico de um objeto. O controle de versão fornece as seguintes funções para controlar a infraestrutura de TI:

Instantâneos

Gravado automaticamente para as mudanças que você fez ao valor de qualquer atualização de um objeto, por exemplo, quando você atualiza um IC. O controle de versão cria um instantâneo que registra o estado completo do IC de hardware depois que o tamanho da memória de um computador é modificado. O controle de versão pode exibir o instantâneo e pode indicar quais atributos do IC foram alterados. O controle de versão também pode compara-lo com todos os outros instantâneos históricos daquele IC. Essas informações são vitais para compreender o impacto de mudanças na disponibilidade e desempenho de um IC.

Marcos

Registrados como instantâneos para finalidade especial com um rótulo definido pelo usuário, como Primeiro dia de produção ou Linha de base de janeiro. Tais rótulos podem ajudar a localizar instantâneos específicos mais rapidamente.

Importante: Marcos *não* se aplicam às especificações de mudança, políticas de verificação, estados de mudança gerenciada e atributos gerenciados.

Comparações

Comparar um IC a outro IC que age como padrão. É possível usar qualquer IC como padrão para fins de comparação; entretanto, recomendamos dedicar ICs específicos à finalidade de atuar como *ICs padrão*. Um IC padrão permite definir uma configuração padrão com a qual outros ICs operacionais na mesma família podem ser comparados. Por exemplo, uma organização pode optar por definir Servidor grande como IC padrão para definir os valores de atributos que definem esse tipo de servidor. O IC padrão de uma família pode ser transformado em um atributo de um IC operacional em tal família, o que permite comparar o estado atual ou qualquer estado histórico de um IC para sua configuração padrão associada. Como outras comparações, é possível imprimir estas informações ou exportá-las como um arquivo delimitado por vírgula.

Embora marcos possam atuar como linhas de bases não compartilhadas e inalteráveis, os ICs padrão fornecem linhas de base dinâmicas compartilhadas aos ICs.

Importante: Um IC padrão nunca deve conter valores para nenhum atributo que seja usado para reconciliação do IC.

Especificações de mudança

Exibir especificações agendadas pendentes ou mudanças não programadas que um usuário especificou em relação a Requisições de mudança do IC. Você pode comparar a especificação de mudança com o estado atual do IC. Por exemplo, a comparação de um valor planejado com o estado atual de um IC. Essa comparação pode mostrar conflitos com as mudanças, identificar mudanças que se sobrepõem no cronograma, e assim por diante.

O controle de versão permite executar as seguintes tarefas:

- Captura automática de todas mudanças em ICs.
- Instantâneos de um IC a qualquer momento com base na data ou em mudanças de atributos.
- Vários níveis de exibição, incluindo exibições detalhadas Log, Básica e Avançada.

- Diversas comparações de atributos com outros instantâneos, marcos definidos pelo usuário ou um IC padrão.
- Instantâneos automáticos sempre que o CA SDM altera os estados de mudança de tickets.

  Observação: este instantâneo automático não se aplica às especificações de mudança, verificação de políticas, estados de mudança gerenciada e atributos gerenciados.
- Filtragem e comparação avançadas com o suporte à impressão e exportação de CSV.

Mais informações:

Usos do Versioning (na página 561)
Ativo compartilhado e registros de trilha de auditoria de IC (na página 562)
Terminologia de versões (na página 563)
Origens de dados de versão (na página 566)
Integração do gerenciamento de mudança do CA SDM (na página 567)
Integração do CA APM (na página 568)
Gerenciamento de controle de versão de IC (na página 569)
Gerenciamento de mudança do CA SDM (na página 588)
CACF (Configuration Audit and Control Facility) (na página 663)
Controle de versão do IC e Estado futuro (na página 690)

Usos do Versioning

O controle de versão inclui os seguintes usos:

Determinação de problemas

Para corrigir o problema com um IC, você *deve* entender o que foi alterado no ambiente do IC. O controle de versão mostra seu estado de defeito atual, além de seu estado em qualquer momento no passado, o que permite comparar os dois estados para ajudar a identificar possíveis problemas.

Planejamento de desempenho e capacidade

Ao revisar o histórico de um IC, um planejador de desempenho ou capacidade está mais apto a determinar as causas dos gargalos de desempenho e planejar o futuro crescimento do sistema.

Conformidade

É possível comparar o estado de um IC com o IC Padrão da sua família. Comparar o estado em qualquer ponto do seu ciclo de vida de gerenciamento de mudança para ajudar a garantir que o IC esteja em conformidade e ajudar a identificar atributos que precisam de correção.

Verificação de mudança

Você pode exibir o histórico de auditoria do objeto, por exemplo, qual usuário modificou uma política de verificação, a data da solicitação, os atributos e valores que o usuário modificou. É possível comparar e contrastar as mudanças entre determinadas datas.

Ativo compartilhado e registros de trilha de auditoria de IC

O recurso Controle de versão inclui mudanças de trilha de auditoria feitas ao CA APM. O recurso Controle de versão também oferece suporte à inicialização em contexto do CA CMDB para o CA APM diretamente de uma entrada de log de atributos associada a cada mudança do CA APM. As informações de trilha de auditoria do CA APM estão disponíveis somente para IC/ativos de famílias do CA CMDB com o log de auditoria do CA APM ativado.

A guia Versioning que inclui as informações da trilha de auditoria do CA APM dá suporte a todas as famílias, desde que o logon para essa família esteja ativado.

Por padrão, o CA APM não registra mudanças de atributo de ativos. Para usar o Controle de versão com um ativo/IC gerenciado pelo CA APM, a opção Armazenar dados de trilha de auditoria deve estar ativada em todos os atributos de ativos que exigem log.

Observação: para obter mais informações sobre como ativar a auditoria, consulte a documentação do CA APM.

Quando atributos de ativo são modificados no CA APM, os dados da guia Controle de versão, na página CI Detail, podem ser atualizados antes dos dados da guia Atributos devido à atividade de armazenamento em cache. Para sincronizar novamente os valores, clique no botão Editar.

Terminologia de versões

A geração de versões é a prática de representar e rastrear *transições de serviço*. A versão normalmente usa uma convenção de nomenclatura para identificar as datas, sequências e significados de tais transições. Esses registros podem ser usados para identificar e comparar estados específicos de um IC (item de configuração).

Exemplo: comparação de versões

Para um IC de aplicativo de folha de pagamento, uma comparação da Versão 3 com a Versão 2 indica os recursos aprimorados e outras diferenças da versão mais recente.

Mais informações:

Estados (na página 563)
Versões (na página 563)
Instantâneos (na página 563)
Categorias (na página 564)
Marcos (na página 564)
ICs padrão (na página 565)

Estados

No contexto de versões, o *estado* de um IC representa todos os valores de atributos de tal IC em um único ponto no tempo. O estado de um IC pode ser o resultado de mudanças em atributos de diversos MDRs.

Versões

Uma *versão* é uma instância identificada de um objeto como um IC dentro da análise de um produto ou da estrutura da configuração. Utilize Versões para fins de rastreamento e auditoria do histórico de mudanças.

Instantâneos

Um *instantâneo* é uma representação do estado completo de um objeto em um único ponto no tempo. Por exemplo, um IC típico possui muitos instantâneos associados a ele. Um instantâneo consolida todos os eventos de modificação que ocorrem com um objeto durante um intervalo de um minuto. Por exemplo, se um IC for atualizado (editado e salvo) diversas vezes em um minuto, o CA SDM cria um único instantâneo que captura todas as atualizações durante esse minuto.

Instantâneo é um termo geral que se refere a instantâneos com base em hora e data, bem como a marcos ou ICs padrão. Para ajudar a localizar pontos significativos no tempo, o CA SDM permite que você identifique os instantâneos de forma significativa. Esses instantâneos nomeados são chamados de marcos.

Toda vez que é feita uma mudança em um objeto, o CA SDM cria um instantâneo automaticamente, sem necessidade de ação manual. O controle de versão captura todas as mudanças ao objeto. Por exemplo, os instantâneos criados usando a interface de usuário, ou instantâneos originados em um MDR e transferidas para o CMDB por meio do GRLoader ou dos Serviços web do CA CMDB.

Categorias

Uma *categoria* identifica uma classe de atributos. A categoria normalmente é o nome da guia que exibe os atributos.

Observação: uma categoria que não é um nome de guia é atribuída a itens que não são encontrados em uma guia (por exemplo, nome, número de série, sinalizador ativo).

Exemplos: Guias e categorias

Os exemplos a seguir mostram como as categorias correspondem a guias:

- Como *Espaço em disco* aparece na guia Atributos, sua categoria é *Atributos*.
- Como *Endereço IP* aparece na guia Inventário, sua categoria é *Inventário*.
- *Marco* aparece na categoria *Geral*.
- Um *IC padrão* aparece na categoria Classificação.
- *Relacionamentos* aparecem na categoria Relacionamento.

Marcos

Um *marco* é um instantâneo rotulado sob demanda de um IC criado para marcar um evento, um ponto de interrupção lógico ou um acúmulo de mudanças. O marco contém o estado real do IC no momento em que o instantâneo foi criado. Marcos permitem identificar e navegar rapidamente até pontos significativos no histórico de um IC. Criar um marco cria um instantâneo "data" equivalente.

Marcos são específicos dos ICs e não são compartilhados. Ao criar um marco para um objeto de alto nível, como um serviço, os subcomponentes de tal objeto de alto nível não criam marcos automaticamente. Para aceitar um marco para um objeto que é composto de diversos subcomponentes, você pode gerar diversos marcos independentes.

Marcos são estáticos e não podem ser alterados ou excluídos. Ao criar um marco, o instantâneo é do estado atual do IC. Posteriormente, quando são exibidos ou usados em uma comparação, os marcos sempre fazem referência a um ponto no passado. Uma boa convenção de nomenclatura para seus marcos ajuda a identificar facilmente pontos cruciais na vida de um IC.

Importante: Marcos *não* se aplicam às especificações de mudança, políticas de verificação, estados de mudança gerenciada e atributos gerenciados.

ICs padrão

Um *IC padrão* é uma configuração abstrata para uma família de ICs que pode ser usada para comparações de linha de base com instâncias de ICs "reais" na mesma família. Um IC padrão pode ser um IC real no sentido de que representa um objeto físico ou pode existir apenas para fins de comparação. ICs padrão possuem as seguintes associações:

- Um IC padrão pode ser compartilhado entre diversos ICs.
- Um IC pode possuir apenas um único IC padrão associado a ele em qualquer momento. Quando o IC padrão é alterado, essa mudança se reflete em todas as comparações entre quaisquer ICs associados e o IC padrão.
- Uma família pode ter diversos ICs padrão. Por exemplo, uma família pode ter ICs padrão chamados “Servidor de teste padrão”, “Servidor de produção padrão”, “Servidor de aceitação padrão”. Recomendamos nomear os ICs padrão de uma forma que eles possam ser facilmente pesquisados e identificados como ICs padrão.

Como um IC padrão é um IC, ele pode ser gerenciado. Ele possui uma trilha de auditoria, segurança, um histórico de mudanças, e assim por diante, como a qualquer outro IC. Após a definição de um IC padrão para um IC específico, é possível usá-lo para verificar a conformidade com os padrões corporativos.

O conceito de "data" ou "hora" não se aplica ao comparar um IC padrão com um instantâneo ou marco. Apenas os valores de atributos do IC padrão são usados para fins de comparação. Instantâneos e marcos específicos do IC padrão não se aplicam.

Exemplo: uso do IC Padrão

Uma empresa define a configuração de uma **Estação de trabalho de funcionário** como o IC padrão para comparar com seus computadores reais na família Hardware.Workstation. Uma comparação revela que um computador específico possui apenas 1 GB de RAM, em vez do valor de memória do IC padrão de 2 GB.

Origens de dados de versão

Os dados de controle de versão são gerados sempre que você criar ou modificar um objeto por qualquer componente que ofereça suporte ao recurso Log de auditoria. Não é possível distinguir instantâneos gerados a partir de diversas origens. Quando o ambiente está configurado adequadamente, os instantâneos aparecem automaticamente sempre que mudanças forem feitas nos ICs e em seus relacionamentos.

Todas as famílias do CA CMDB estão ativadas para controle de versão. ICs em famílias base do CA Service Desk devem ser convertidas em famílias do CA CMDB para aproveitar as vantagens do controle de versão.

Dados de controle de versão incluem as seguintes origens:

- **Atualizações de ICs do CA CMDB** – atualizações de atributos comuns de ICs e atributos de ICs específicos de famílias usando a interface de usuário.
- **Atualizações de relacionamentos do CA CMDB** – atualizações de relacionamentos na guia Relacionamentos e na Lista de relacionamentos de ICs usando os recursos Editar e Editar na lista.
- **GRLoader** - Atualizações de inserções e atributos de ICs, atualizações de relacionamentos, atribuições de ICs padrão e marcos importados usando o GRLoader. Quando atualizações de um MDR são enviadas usando o GRLoader, a origem do MDR também é registrada, permitindo rastrear mudanças de atributos diretamente à sua origem.

  Observação: para obter mais informações, consulte o *Guia de Referência Técnica*.
- **Histórico de mudança do CA SDM** —um instantâneo é automaticamente criado para todos os ICs associados a um ticket de mudança. Até quatro instantâneos são gerados quando o IC é aberto, fechado, ativado ou resolvido.

- **Mudanças de IC do CA APM (CA Asset Portfolio Management)**—mudanças feitas pelo CA APM a ICs com geração de logs ativada.
- **Verificação de mudança:** atualiza para especificações de mudança, políticas de verificação, estados de mudança gerenciada e atributos gerenciados.

Observação: os ICs criados no CA SDM ou releases anteriores do CA CMDB contêm apenas mudanças de modificação. Valores de atributos iniciais, como nome, família e classe, não foram registrados e não aparecem nos instantâneos. Além disso, os relacionamentos criados com o CA Service Desk ou versões anteriores do CA CMDB não possuem informações do histórico de auditoria.

Integração do gerenciamento de mudança do CA SDM

Os dados de controle de versão são gerados para cada IC associado ao ticket de mudança do CA SDM. À medida que o ticket de mudança passa de aberto para ativo para resolvido para fechado, é capturado um instantâneo para cada um dos ICs associados. Assim, instantâneos são criados para os status de aberto, fechado, ativo ou resolvido. Se não houver ICs associados a uma requisição de mudança, nenhum instantâneo é gerado.

Observação: o recurso de controle de versão não exige nenhuma configuração especial e é suportado automaticamente em instalações integradas.

O recurso de controle de versão trata do ticket de mudança como segue:

1. Compara o estado do IC no momento em que o ticket foi aberto com seu estado atual.
2. Verifica se todas as mudanças obrigatórias foram adequadamente executadas e se nenhuma mudança adicional foi introduzida.
3. Fecha o ticket após as mudanças terem sido validadas.

Para fins de auditoria, é possível comparar prontamente o estado do IC antes e depois de cada mudança ser feita. As informações de comparação ajudam a responder perguntas sobre o estado de um IC antes e depois de uma requisição, por exemplo:

- A mudança apropriada ocorreu conforme o solicitado?
- Quais outras mudanças ocorreram no IC não relacionadas ao ticket de mudança?
- A que horas as mudanças ocorreram?
- Qual é a diferença entre o IC e a configuração padrão, tanto antes quanto depois da mudança?

Integração do CA APM

O controle de versão exibe mudanças feitas pelo CA APM a seus ICs. O controle de versão também oferece suporte à execução no contexto do CA CMDB para o CA APM diretamente de qualquer entrada de log de atributo que esteja associada a uma mudança do CA APM. Informações de auditoria do CA APM estão disponíveis apenas para ICs de famílias do CA CMDB quando a geração de logs de auditoria do CA APM está ativada.

Observação: quando atributos de IC são modificados no CA APM, os dados da guia Controle de versão na página CI Detail podem ser atualizados antes dos dados da guia Atributos devido à atividade de armazenamento em cache. Para sincronizar novamente os valores, clique no botão Editar.

Por padrão, o CA APM não registra mudanças de atributos de ICs. Para usar o Controle de versão com um IC gerenciado pelo CA APM, a opção Store Audit Trail Data deve estar ativada em todos os atributos de ativos que exigem geração de logs.

Por padrão, há um atraso de dez minutos entre o momento em que um IC é atualizado no CA APM e o momento em que ele fica disponível para o controle de versão no CMDB. É possível modificar esse atraso alterando a variável @NX_DBMONITOR_TIMER_MINUTES em uma instalação integrada.

Observação: para obter informações sobre como ativar a geração de logs de atributo para ativos, consulte a documentação do CA APM.

Mais informações:

Recursos de integração do CA APM (na página 568)

Recursos de integração do CA APM

O CA SDM fornece os seguintes recursos de integração com o CA APM:

- Registros compartilhados e log de auditoria que diferenciam entre ativos e ICs do CA APM
- Execução em contexto do CA CMDB e CA APM para informações de IC/ativo
- Campos de tabela de extensão compartilhados
- Um contato do CA SDM atualiza quando o CA APM altera um contato principal
- Modificação do tipo de ativo do CA APM para usar famílias do CI

Gerenciamento de controle de versão de IC

É possível exibir e gerenciar o histórico do IC, instantâneos associados, marcos, mudanças não agendadas e outras exibições. Você usa a seção esquerda para navegar e a direita para exibir os detalhes do IC e o log de auditoria.

Observação: o controle de versão funciona da mesma forma em relação ao histórico de atributos gerenciados e ao histórico de estado de mudanças gerenciadas. Por exemplo, a guia Histórico do atributo gerenciado exibe informações de controle de versões sobre um atributo gerenciado.

Use as informações do controle de versão para identificar as especificações de mudança e Requisições de mudanças associados. O controle de versão identifica mudanças não agendadas nas especificações de mudança na exibição do instantâneo que corresponde às requisições de mudança sem data de início programada. Você pode exibir o instantâneo e o log de uma especificação de mudança no CACF.

Exemplo: mudança não agendada

Nesse exemplo, um usuário tenta alterar o valor de um atributo gerenciado. É possível exibir a guia Controle de versão na página Detalhes do IC, que exibe a mudança não agendada no instantâneo. Esse instantâneo exibe informações sobre a mudança, como data, hora, nome de usuário, e o valor do atributo.

Ao selecionar um instantâneo ou marco na seção esquerda, a seção direita exibe os valores de atributo do estado, evento ou comparação desse IC. A seção esquerda pode exibir instantâneos ou marcos do IC por data e hora (modo Básico) ou por características do IC (modo Avançado), e inclui os seguintes links para ajudar a gerenciar um IC:

Criar marco

Rotula o estado do IC.

Mostrar log

Exibe o histórico do IC não filtrado.

Advanced/Basic

Alterna entre exibições de instantâneo.

Ocultar valores vazios

Permite filtrar os campos de dados em branco. Quando não selecionado, todos os atributos do IC são exibidos.

Print and Export

Imprimir ou cortar e colar para salvar os dados de controle de versão na exibição.

Mostrar log

O log permite exibir o histórico do item de configuração. A opção Filtro permite filtrar linhas do log. As opções Print (Imprimir) e Export (Exportar) permitem imprimir ou recortar e colar para salvar o dados de versão em exibição.

O painel de informações do Versioning exibe os seguintes campos:

- Categoria
- Data
- Log
- Atributo
- Valor novo
- Valor antigo
- Mudança feita por
- MDR

Observação: o log exibe apenas as *atualizações* de atributos de ICs criados em releases anteriores do CA SDM ou CA CMDB. Não exibe seus valores de atributos iniciais de ICs. Relacionamentos criados em releases anteriores do CA SDM CA CMDB não incluem informações do histórico de auditoria e não aparecem no log.

Filtragem de log

O log pode ser filtrado digitando uma sequência de caracteres simples no campo Filtro. O Filtro diferencia letras maiúsculas de minúsculas. Se a sequência de caracteres do filtro aparecer em qualquer lugar de uma linha do log, a linha é exibida. Não são usados caracteres especiais ou curingas no filtro. As linhas do log que correspondem aos critérios de filtragem são exibidas ocultando as linhas que não correspondem.

Não é necessário pressionar Enter ou atualizar para atualizar a exibição. A exibição do log é filtrada conforme cada tecla é pressionada e aplica-se a todos os campos: Data, Log, Atributo, Valor antigo, Novo valor, MDR e Nome.

Exibir o histórico do item de configuração

Você pode exibir o histórico de um item de configuração.

Para exibir o histórico de um item de configuração

1. Pesquise e abra o item de configuração.

   A página Detalhe de item de configuração aparece.

2. Clique na guia Versão.

   A página Controle de versão é exibida.

3. Clique em Mostrar log.

   O histórico do item de configuração é relacionado.

   Observação: a opção Mostrar log ignora as seleções no painel esquerdo.

Imprimir um log de IC

É possível imprimir o log de um IC.

Para imprimir o log de um IC

1. Selecione um IC e clique na guia Versão.
2. Clique no link Mostrar log.
3. (Opcional) Digite os critérios de filtro desejados para ocultar/mostrar linhas de log.
4. Clique em Imprimir.

   É exibida uma janela fácil para impressão. O relatório Versão do IC é exibido.
5. Use a janela do navegador web para clicar em Arquivo, Imprimir para imprimir uma cópia do relatório.

   O texto formatado é enviado à impressora definida.

Suporte à exportação de CSV

É possível exportar o conteúdo de log do CA CMDB para um arquivo no formato CSV que aplicativos ou ferramentas de relatório de terceiros podem importar. A exportação possui base no que está em exibição no momento, que pode estar filtrado ou não.

Mais informações:

Exportar dados (na página 584)

Logs integradas do CA SDM e CA APM

Além das mudanças feitas usando as instalações CA CMDB, o log do IC também inclui eventos de atualização de atividades do ticket de mudanças CA SDM e atualizações do CA APM.

Mais informações:

Integração do CA APM (na página 568)

Início no contexto e identificação de origens de MDRs

O CA CMDB fornece uma forma de início no contexto, diretamente do log para o provedor de dados do MDR para uma entrada de log específica do IC. Você também pode iniciar no contexto para a especificação da mudança. Esse recurso de inicialização faz o seguinte:

- Rastreia mudanças em atributos até o MDR de origem, quando o MDR usou as marcas <mdr_name> <mdr_class> e <federated_asset_id> na entrada do GRLoader.

  Observação: para obter informações, consulte o *Guia de Referência Técnica do CA CMDB*.

- Identifica quando um atributo do IC está sendo atualizado por mais de um MDR. Essa situação ocorre quando diversos MDRs contribuem com dados independentemente para uma definição de IC.
- Identifica qual MDR está atuando como a origem de autorização.

Observação: entradas de log criadas no CA SDM ou releases anteriores do CA CMDB não contêm informações com o contexto da inicialização do MDR. Além disso, o CA Cohesion ACM fornece informações de início de MDRs para a maioria dos atributos ou relacionamentos, mas todos.

Nomes de atributos

Os nomes de atributos exibidos no log agora correspondem ao nome de atributo exibido na interface de usuário; eles não refletem mais o nome do objeto interno. Por exemplo, o CA CMDB exibe “Tipo de manutenção” em vez de “mtce_type”.

Geração de logs de famílias e atributos personalizados

Para permitir a geração de log para famílias e atributos personalizados, especifique novos atributos de MDR e acionadores de auditoria. Se você criar novas famílias ou atributos, deve criar também arquivos de metadados para especificar nomes de atributos legíveis por humanos para exibição no log; caso contrário, o nome do objeto interno aparecerá.

Observação: para obter mais informações, consulte Extensão do CA CMDB no *Guia de Administração*.

Criar um marco

É possível criar um marco a partir da interface com o usuário ou usando o GRLoader.

Para criar um marco na interface de usuário

1. Selecione um IC e clique na guia Versão.
2. Clique em Create Milestone (Criar marco).
3. Digite um texto descritivo para o marco. Clique em Salvar.

   A janela Criar marco é fechada.

4. Selecione Exibir, Atualizar.

   A exibição Básica mostra um novo instantâneo, com a data e a hora atuais, que representa o marco criado. Alternar para a exibição Marco mostra apenas os instantâneos com nomes atribuídos. Os marcos são exibidos em uma sequência de data/hora decrescente, com o mais recente na parte superior.

Para criar um marco usando o GRLoader

1. Adicione a marca <milestone> ao XML para esse IC.
2. Aplicam-se as mesmas regras de reconciliação que ao associar um marco a um IC.

   Observação: o valor da marca marco é o rótulo associado ao marco.

3. Salve e feche o XML para o IC.

   O marco é criado.

Observação: para obter informações, consulte o *Guia de Referência Técnica do CA CMDB*.

Exemplo: use o GRLoader para criar um marco

O exemplo a seguir do GRLoader cria o marco **Fim do ano fiscal de 2008**.

```
<ci>
<name>server1 </name>
<milestone>Fim do ano fiscal de 2008</milestone>
</ci>
```

Criar um IC padrão

Crie um IC padrão da mesma forma que cria qualquer outro IC.

Para criar um IC padrão na interface de usuário

1. Selecione Criar novo item de configuração no menu Arquivo.
2. Selecione a família que deseja usar para o novo IC padrão.
3. Defina os atributos como com qualquer IC normal.

   O IC padrão é criado.

Observação: qualquer IC pode atuar como um IC padrão, mas os seguintes cuidados devem ser observados:

- Um IC padrão deve seguir uma convenção de nomenclatura para que ele não seja confundido com ICs normais.
- Um IC padrão deve atuar apenas como uma linha de base para ICs na mesma família do IC padrão.
- *Não* devem ser atribuídos valores a um IC padrão para nenhum atributo usado em reconciliação; por exemplo, Endereço MAC, Número de série, ID do IC alt., DNS, etc.
- Como os ICs padrão são indistinguíveis de ICs normais, eles aparecem no Gerenciador de filas e no número total de ICs.
- É melhor um IC padrão não representar uma instância real de um objeto comercial.

Atribuir um IC padrão a um IC

Você pode atribuir um item de configuração padrão a um item de configuração usando a página Detalhes do IC. Você pode atribuir um IC padrão a uma lista de ICs ou usando Editar na Lista.

Para atribuir um IC padrão da família a um IC usando a página Detalhes do IC

1. Selecione um IC e clique em Editar.

   A página Atualizar item de configuração aparece.

2. Clique no ícone ao lado do campo IC padrão.

   A Lista de ICs é exibida.

3. Selecione um IC para servir como o IC padrão. Clique em Salvar.

   O IC padrão é atribuído.

Para atribuir ICs padrão a uma lista de ICs usando a opção Editar na lista

1. Na guia Placar ou Administração, especifique o filtro de pesquisa para mostrar um único IC ou diversos ICs na lista de detalhes e clique em Pesquisar.

   Os ICs que corresponderem aos critérios de pesquisa são relacionados.

2. Clique no botão Editar na lista no canto superior direito dos resultados da lista.

   Os controles de Editar na lista de ICs são exibidos.

3. Selecione uma linha que contenha o IC para atribuir o IC padrão.

   A linha é exibida numa cor realçada.

4. Clique no ícone ao lado do campo IC padrão.

   A Lista de ICs é exibida.

5. Selecione um IC para servir como o IC padrão. Clique em Salvar para atualizar o único IC ou em Alterar tudo para atualizar todos os ICs na lista.

   O IC padrão é atribuído ao único IC (Salvar) ou a todos os ICs relacionados (Alterar tudo).

Observação: qualquer IC pode atuar como um IC padrão, mas os seguintes cuidados devem ser observados:

- Um IC padrão deve seguir uma convenção de nomenclatura para que ele não seja confundido com ICs normais.
- Um IC padrão deve atuar apenas como uma linha de base para ICs na mesma família do IC padrão.
- *Não* devem ser atribuídos valores a um IC padrão para nenhum atributo usado em reconciliação; por exemplo, Endereço MAC, Número de série, ID do IC alt., DNS, etc.
- Como os ICs padrão são indistinguíveis de ICs normais, eles aparecem no Gerenciador de filas e no número total de ICs.

É melhor um IC padrão não representar uma instância real de um objeto comercial.

Atribuir um IC padrão a um IC usando o GRLoader

Para atribuir um IC padrão a um IC, inclua a marca <standard_ci> na descrição de um IC.

Observação: para obter informações, consulte o *Guia de Referência Técnica do CA CMDB*.

Exemplo: atribuir um IC padrão a um IC

Caso tenha uma configuração padrão de estação de trabalho armazenada em um IC chamado **configuração padrão de estação de trabalho**, é possível atribuir esse IC padrão à Estação de trabalho do Joe usando o GRLoader para carregar o seguinte XML:

```
<ci>
        <name>Estação de trabalho do Joe</name>
        <class>Servidor</class>
        <standard_ci>configuração padrão de estação de trabalho</standard_ci>
</ci>
```

Usar a exibição básica

Você pode selecionar instantâneos em exibição Básica ou Avançada; os mesmos tipos de dados de controle de versão podem ser exibidos em ambos os modos. A exibição Básica permite facilmente visualizar o estado de um IC.

Para usar a exibição Básica para visualizar o estado de um IC.

1. Abra o IC na interface de usuário e clique na guia Controle de versão.

   Os instantâneos existentes são listados do lado esquerdo da página.

2. Selecione um tipo de instantâneo na lista suspensa de tipo de Instantâneo.

   Observação: se um IC padrão estiver especificado para o IC focal, ele é exibido na parte superior da lista de instantâneos ou marcos e identificado por um indicador IC padrão à direita do nome do IC. Se você clicar em um IC padrão, os atributos para o IC padrão são exibidos, e não o IC focal.

   Instantâneo

   Lista todos os instantâneos do IC identificados com base na data/hora e no IC padrão. Essa é a opção padrão.

Marco

Lista todos os Marcos definidos pelo usuário e o IC padrão.

O estado de um IC é exibido na seção direita.

A área de texto informativo na parte inferior exibe informações do item sobre o qual o ponteiro do mouse está posicionado no momento. Passar o cursor sobre um instantâneo, marco ou IC padrão mostra informações sobre a data e a hora de criação e o tipo de instantâneo.

Observação: você pode selecionar dois ou mais instantâneos, marcos ou ICs padrão para compará-los.

Usar a exibição avançada

Você pode selecionar instantâneos em exibição Básica ou Avançada; os mesmos tipos de dados de controle de versão podem ser exibidos em ambos os modos. A exibição avançada permite instantâneos com base no tipo de atributo, valor e marca de data e hora. A exibição avançada também permite quaisquer comparações com atributos, marcos ou um IC Padrão. Uma hierarquia de árvore mostra uma pasta para cada atributo do IC, e cada pasta de atributo contém um histórico dos valores do atributo. A hierarquia é organizada desta forma:

```
Raiz
    Nome do atributo
        Valor do atributo1:
        Valor do atributo2:
```

Essa hierarquia permite visualizar o histórico de valores únicos para qualquer atributo em particular em resumo.

Para usara exibição Avançada

1. Abra o IC na interface de usuário e clique na guia Controle de versão.

   Os instantâneos existentes são listados do lado esquerdo da página.

2. Clique em Avançado.

   Seleção avançada mostra uma hierarquia de pasta.

3. Navegue para a hierarquia de pasta e clique na pasta que inclui as informações que deseja ver:

   Data

   Lista Instantâneos com base em data/hora, o que é idêntico à exibição Básica. Os instantâneos podem ser subdivididos adicionalmente com base no ano/mês se houver 30 ou mais instantâneos para o IC. O IC padrão também é relacionado nessa pasta se um foi atribuído ao IC de foco.

   Marco

   Lista todos os marcos definidos pelo usuário, o que é idêntico à exibição Básica. O IC padrão também é relacionado nessa pasta se um foi atribuído ao IC de foco.

   Os atributos do IC padrão são exibidos como nós especiais de folhas da árvore com um IC padrão. Os valores do IC padrão aparecem apenas para atributos para os quais houver um valor de IC padrão. Eles não aparecem para atributos em que o valor não foi definido.

   Relacionamento

   Contém todos os relacionamentos (passados e presentes) para o IC. A hierarquia de pastas transmite as seguintes informações:

```
Relacionamento
     Tipo de relacionamento
          IC de parceiro
               Status e Data
```

Tipo de relacionamento especifica o tipo de relacionamento, como “está em”, “hospeda” ou “comunica-se com”.

O IC de parceiro é o nome do IC associado ao relacionamento.

Status e Data especificam o status do relacionamento na data e hora especificadas. O valor de status inclui os seguintes:

- Relacionamento criado – O estado do IC quando o relacionamento foi criado.
- Relacionamento finalizado – Esse IC não está mais envolvido no relacionamento. O relacionamento ainda existe na extremidade do parceiro, mas o IC de foco não está envolvido.
- Relacionamento excluído - O relacionamento foi marcado como excluído.
- Relacionamento alterado - O relacionamento foi reativado a partir do estado excluído.
- Novo parceiro e tipo – A extremidade do parceiro do relacionamento foi atribuída a um novo IC e o tipo de relacionamento foi alterado ao mesmo tempo.
- Novo tipo de relacionamento - O tipo de relacionamento entre dois ICs foi alterado.
- IC de parceiro atribuído – A extremidade do parceiro do relacionamento foi alterada.

4. Clique em um valor de atributo.

   O estado completo do IC no momento em que o valor de atributo foi definido é exibido.

Exemplo: use a exibição avançada para mostrar atributos de espaço em disco

No exemplo a seguir, a seleção avançada mostra que o espaço em disco aumentou de 10 a 20 para 100 GB.

```
Raiz
      Espaço em disco
            10 GB
            20 GB
            100 GB
```

Clique em qualquer valor para ver quando a mudança ocorreu, o estado dos outros atributos quando a mudança ocorreu e o número da requisição de mudança aberta quando o espaço em disco foi alterado.

Exibir detalhes de instantâneo

Você pode exibir detalhes do instantâneo na exibição Básica ou Avançada. Por exemplo, a exibição básica mostra um instantâneo de uma mudança não agendada para um IC.

Para exibir detalhes do instantâneo

1. Abra o objeto na interface de usuário e clique na guia Controle de versão.

   É exibida uma lista dos instantâneos existentes no lado esquerdo da página.

2. Clique em um instantâneo.

   Detalhes são exibidos na seção direita das exibições Básica e Avançada. Quando apenas um item é selecionado, a seção direita mostra as informações sobre o instantâneo, marco (somente em relação a ICs) ou padrão selecionado.

   Os dados exibidos incluem os detalhes e indicadores a seguir:

   Ocultar valores vazios

   Permite filtrar os campos de dados em branco. Quando essa opção está desmarcada, todos os atributos do IC são exibidos.

   Texto do campo Valor em negrito

   Indica que um atributo ou relacionamento foi alterado desde que o último instantâneo foi feito. Ao exibir detalhes de um IC padrão, todos os valores estão em negrito.

   Valor

   Mostra o valor anterior do atributo e a hora da última mudança quando você passa o cursor sobre o valor. As informações são exibidas na área de texto na parte inferior da guia Controle de versão.

   Valor “(em branco)”

   Indica se um valor anterior foi desmarcado.

Categoria de relacionamento

Mostra informações sobre o relacionamento, incluindo informações de IC de parceiro e tipo.

Início no contexto e identificação de origens de MDRs

Proporciona início no contexto de um MDR provedor a partir da entrada de detalhes do IC.

Observação: em ICs criados no CA SDM ou em versões anteriores do CA CMDB, informações do MDR e de Alterado por podem estar ausentes. Além disso, o CA Cohesion ACM fornece início no contexto de MDRs para a maioria dos atributos ou relacionamentos, mas todos.

Rastreia mudanças nos atributos de volta para o MDR de origem.

Detecta quando um atributo do IC é atualizado por mais de um MDR. Essa situação ocorre quando diversos MDRs contribuem com dados independentemente para uma definição de IC.

Identifica qual MDR atua como a origem de autorização.

Exibir o estado de um IC em uma data específica (exibição Básica)

É possível usar a exibição básica para ver o estado de um IC em uma data específica.

Para exibir o estado de um IC em uma data específica

1. Selecione um IC e navegue até a página Detalhes do IC.
2. Clique na guia Versão.

   A exibição Basic (Básica) do IC é mostrada.
3. Selecione a data desejada.

   O lado direito da exibição mostra o estado do IC na data selecionada.

Exibir o estado de um IC em uma data específica (exibição avançada)

É possível usar a Seleção avançada para exibir o estado de um IC em uma data específica.

Para exibir o estado de um IC em uma data específica

1. Selecione um IC e navegue até a página Detalhes do IC.
2. Clique na guia Controle de versão e clique em Avançado.

   A árvore Advanced Selection (Seleção avançada) é exibida.
3. Expanda a pasta Data.
4. Selecione a data na qual deseja exibir o IC.

   O estado do IC nessa data é exibido.

Iniciar o MDR que definiu um atributo

Se o histórico para um IC faz referência a um MDR, é possível iniciar um MDR para exibir os detalhes do IC.

Para iniciar um MDR para exibir detalhes do IC

1. Selecione um IC e navegue até a página Detalhes do IC.
2. Clique na guia Versão.
3. Clique em Exibir log ou selecione o marco ou instantâneo do IC que deseja exibir.
4. Selecione a linha do atributo que deseja investigar.
5. Se o histórico do IC faz referência a um MDR, clique no link MDR.

   O MDR provedor mostra detalhes adicionais do IC.

Imprimir um instantâneo

É possível imprimir um instantâneo de uma data selecionada.

Siga estas etapas:

1. Selecione o objeto e clique na guia Controle de versão.
2. Selecione a exibição Basic (Básica).
3. Selecione um Instantâneo na lista suspensa de tipo de Instantâneo.
4. Selecione a data na lista de datas à esquerda.

5. Clique em Imprimir.

   Aparece uma janela de impressora amigável que exibe o relatório do Controle de versão para o IC.

6. Use a janela do navegador web para clicar em Arquivo, Imprimir para imprimir o relatório.

   O texto formatado é enviado à impressora definida.

Imprimir um marco de IC

É possível imprimir um marco de um IC a partir de uma data selecionada

Para imprimir um marco de um IC a partir de uma data selecionada

1. Selecione um IC e clique na guia Versão.
2. Selecione o marco desejado na exibição Básica ou Avançada.
3. Clique em Imprimir.

   É exibida uma janela para impressão que exibe o relatório de controle de versão para o IC.

4. Use a janela do navegador web para clicar em Arquivo, Imprimir para imprimir o relatório.

   O texto formatado é enviado à impressora definida.

Exportar dados

A página Versioning Export to CSV permite exportar o instantâneo e as informações de log em um formato CSV (comma separated value - valor separado por vírgula). Os dados são exibidos em uma página Exportar. Os dados formatados correspondem à exibição obtida, com linhas exibidas em linhas separadas e valores de colunas separados por vírgula entre aspas duplas. Filtragem e comparação de dados selecionadas na guia Controle de versão é o que está formatado para exportação.

Para exportar dados do IC

1. Selecione o objeto e clique na guia Controle de versão.
2. Clique na exibição desejada do IC.

   Por exemplo, clique em Show Log (Mostrar log), uma comparação de instantâneos, marco (ICs), e assim por diante.

3. Clique em Exportar.

   A opção Export Log (Exportar log) ao CSV para a página IC é exibida.

4. Use a ação Selecionar tudo (a partir do menu de contexto ou do atalho no teclado).

5. Use recortar e colar para transferir os dados da página formatada para um arquivo CSV ou aplicativo de terceiros. Por exemplo, é possível exportar para uma planilha do Excel.

   Os dados são exportados.

Mudanças e instantâneos de família de IC

Mudanças de família podem afetar um instantâneo do IC.

Um instantâneo inclui os seguintes tipos diferentes de atributos:

- Atributos comuns
- Atributos específicos de família

Ao alterar a família de um IC, as seguintes mudanças de instantâneo ocorrem:

- Atributos específicos de família associados à mudança do IC.
- Os detalhes do instantâneo refletem a família no momento do instantâneo.

A família de um IC determina os atributos do IC. Se você alterar o atributo *específico de família* e, em seguida, alterar a família do IC, o resultado é um IC que não mais processa o atributo *específico da família* alterado. Alterar a família de um IC não tem impacto sobre seus atributos *comuns*.

Exemplo: alterar a família associada ao IC

Esse exemplo mostra como mudanças de família do IC afetam um instantâneo do IC.

Tempo	Status/Mudanças
0	O IC está na Família1.
1	Um valor de atributo específico da Família1 é alterado.
2	Diversos valores de atributos comuns são alterados.
3	A família do IC é alterada de Família1 para Família2. Quando isso ocorre, todos os atributos específicos da Família1 se tornam indisponíveis para o CI.
4	Um valor de atributo específico da Família2 é alterado.

5	Diversos atributos comuns são alterados.
6	A família do IC é alterada de volta para Família1. Quando isso ocorre, todos os valores de atributos específicos da Família2 se tornam indisponíveis para o IC, mas os valores de atributos anteriores específicos da Família1 são restaurados.
7	Diversos atributos comuns são alterados.
8	Um atributo específico da Família1 é alterado.

No exemplo, um instantâneo em Tempo=7 não contém as informações das mudanças feitas nos Tempos 3 ou 4. Essas mudanças representam as mudanças feitas nos atributos específicos da Família2.

Comparar instantâneos (exibição básica)

Você pode comparar dois ou mais instantâneos, marcos, ou ICs padrão.

Para comparar instantâneos, marcos ou ICs padrão

1. Selecione um IC e navegue até a página Detalhes do IC.
2. Clique na guia Versão.
3. Selecione um marco ou instantâneo na lista suspensa de tipo de instantâneo.

   Marcos ou instantâneos são listados.
4. Selecione dois ou mais instantâneos, marcos ou ICs padrão.

   A exibição de comparação mostra os seguintes resultados:

   - A coluna A mostra como os instantâneos ou marcos diferem.
   - Cada linha exibe os valores de atributos dos instantâneos selecionados.
   - Apenas atributos com diferenças são exibidos. A data sempre é exibida, a menos que os instantâneos sejam idênticos.
   - As comparações de IC padrão não tem horário específico, assim seus campos de Data são configurados para dizer **IC Padrão**.
   - Os resultados da comparação podem ser impressos ou exportados para um arquivo CSV.

Comparar instantâneos (exibição avançada)

Você pode comparar dois ou mais instantâneos, marcos, ou ICs padrão.

Para comparar instantâneos, marcos ou ICs padrão na exibição Avançada

1. Selecione um IC e navegue até a página Detalhes do IC.
2. Clique na guia Controle de versão e clique em Avançado.

   A Seleção avançada exibe o IC.
3. Navegue na hierarquia de pastas até o valor que deseja usar para a comparação de instantâneo.
4. Selecione um valor para cada comparação de instantâneo.

   A comparação para o IC é exibida. Por exemplo: uma comparação de instantâneos com base nos valores de pastas selecionados.

   A exibição de comparação mostra os seguintes resultados:

   - A coluna A mostra como os instantâneos ou marcos diferem.
   - Cada linha exibe os valores de atributos dos instantâneos selecionados.
   - Apenas atributos com diferenças são exibidos. A data sempre é exibida, a menos que os instantâneos sejam idênticos.
   - As comparações de IC padrão não tem horário específico, assim seus campos de Data são configurados para dizer **IC Padrão**.
   - Os resultados da comparação podem ser impressos ou exportados para um arquivo CSV.

Observação: na exibição Avançada, dois ICs podem ter um relacionamento sem um tipo de relacionamento atribuído (por exemplo, ICs criados pelo CA NSM). Esses nós de relacionamento são identificados como (em branco).

Gerenciamento de mudança do CA SDM

Os dados de controle de versão são gerados automaticamente para cada IC associado a um ticket de mudança do CA Service Desk. À medida que o ticket de mudança passa de aberto para ativo para resolvido para fechado, é capturado um instantâneo para cada um dos ICs associados. O controle de versão permite fazer o seguinte:

- Comparar o estado do IC com o seu IC padrão em qualquer ponto no ciclo de vida de um gerenciamento de mudança.
- Ajudar a garantir que o IC esteja em conformidade e ajudar a identificar os atributos que precisam de solução de problemas.
- Realizar comparações entre estados do IC em qualquer ponto do ciclo de vida da requisição de mudança, mas também em qualquer data ou horário nesse período.
- Visualizar o progresso em cada estágio da mudança, incluindo quaisquer marcos.

A integração entre o CA Service Desk e o CA CMDB é ilustrada demonstrando como é possível auditar mudanças realizadas durante o ciclo de vida de gerenciamento de serviço de um IC. Neste exemplo, uma requisição de mudança é usada para atualizar componentes de um servidor de hardware.

Para criar uma requisição de mudança e associá-la a um IC

1. Crie um ticket de mudança do CA Service Desk clicando em Arquivo, Nova requisição de mudança.
2. Insira as informações da requisição de mudança e resumo da requisição, por exemplo: atualizar disco rígido para 500 GB.
3. Clique na guia Itens de configuração e, em seguida, clique em Atualizar ICs.
4. Especifique os critérios de pesquisa de ICs (por exemplo, o nome do servidor de hardware) e clique em Pesquisar.
5. No formulário Affected Configuration Items Update, selecione os ICs associados ao ticket de mudança (por exemplo, o servidor de hardware da Etapa 4) adicione-os à lista Itens de configuração afetados. Clique em OK.
6. Salve a requisição de mudança.

Para executar as mudanças

1. Faça mudanças ao IC. Por exemplo, execute a instalação do disco rígido no computador físico e atualize o atributo Capacidade do disco para o IC de servidor de hardware.
2. Feche a requisição de mudança.
3. Certifique-se de que a mudança foi concluída. Visualize o IC, clique na guia Controle de versão e compare os instantâneos do IC antes e depois da mudança.

   Uma comparação do estado do IC entre os horários em que a requisição de mudança foi aberta e fechada mostra que o tamanho do disco rígido do servidor de hardware era de 100 GB antes da mudança, de 500 GB após a mudança ser concluída e a data e horário em que as mudanças ocorreram. Quaisquer outros atributos modificados entre os horários de abertura e fechamento também são exibidos.

Exibir atributos de IC em outros produtos CA

É possível usar a página Common Asset Viewer para exibir atributos de item de configuração em outros produtos da CA.

Para exibir os atributos de itens de configuração em outros produtos da CA

1. Localize a abra o item de configuração.
2. Clique em Visualizador de ativos.

   A página Common Asset Viewer é exibida.
3. Clique nos links na guia Recursos proprietários para localizar as informações de atributos de outros produtos da CA.
4. Clique em Fechar janela ao concluir.

   Você exibiu atributos do item de configuração em outros produtos da CA.

Usando o visualizador do CMDBf

O CA SDM fornece o Visualizador do CMDBf para exibir os resultados da federação do IC através de MDRs. A partir da página CI Detail (ou do menu ao clicar com o botão direito do mouse no IC na Lista de ICs), clique no Visualizador do CMDBf para visualizar os atributos do IC de MDRs e CMDBs federados em paralelo. Na página Federated View, é possível clicar em Recuperar para atualizar as informações de qualquer um dos MDRs federados. Para melhorar a legibilidade, os arquivos de metadados do CA CMDB podem reconciliar os nomes de atributo do MDR e do CA CMDB.

Observação: esse recurso requer MDRs que ofereçam suporte a Consulta. Você configura MDR CMDBf Endpoints para exibir seus resultados em Federated View. Para obter mais informações, consulte o *Guia de Implementação*.

Se o IC não tem nenhum dado federado, o visualizador exibe somente atributos do CA CMDB.

CMDB Visualizer

O CA SDM permite alinhar seus componentes de TI (*itens de configuração* ou ICs) aos serviços de negócio. O CA CMDB define *relacionamentos* entre ICs, como quando um grupo de ICs trabalha para fornecer um serviço de negócio. O CMDB Visualizer permite visualizar todo o panorama de relacionamentos de IC e oferece funções para gerenciar os relacionamentos. Trabalhando a partir de um *IC de foco* (qualquer IC de interesse), é possível usar o Visualizer para exibir até nove níveis de ICs relacionados.

A CA usa um modelo provedor/dependente para definir relacionamentos entre ICs. Todos os ICs que contribuem para um serviço comercial são *provedores* de tal serviço (o *dependente*). De uma forma muito similar, provedores também podem ser *dependentes* que contam com outros ICs. É possível usar o Visualizer para realizar as seguintes análises de provedor/dependente:

Procurar

Mostra uma exibição não filtrada de todos os ICs.

Análise de impacto

Inicia com um IC focal (provedor) e pesquisa seus dependentes.

Motivo raiz

Inicia com um serviço de negócio (dependente) e visualiza todos os ICs que são provedores desse serviço.

ICs de causa e efeito

Combina análise de impacto e causa raiz em uma pesquisa.

Rastrear relação

Exibe todos os relacionamentos possíveis com base em níveis. Se você selecionou somente um IC, esse filtro mostra a exibição Procurar.

Caminho mais curto

Exibe a cadeia mais curta de relacionamentos com base em níveis.

O CMDB Visualizer permite realizar as seguintes ações:

- Visualizar diversos níveis dos ICs a partir de uma exibição gráfica configurável
- Monitorar ou cancelar o processo de criação
- Pesquisar usando critérios flexíveis
- Filtrar com base nas famílias, tipos de relacionamentos e outros atributos do IC
- Exibir relacionamentos do IC
- Acompanhar um relacionamento entre dois ICs.
- Visualizar uma cadeia de dependências
- Chamar o CA CMDB diretamente a partir do Visualizer
- Exibir atributos e propriedades de ICs.
- Salvar os metadados do gráfico
- Imprimir o layout do gráfico
- Localizar um IC específico em um gráfico exibido.
- Criar um IC (dependendo da função)
- Criar novos relacionamentos de IC (dependendo de função)
- Usar o Bloco de anotações para armazenar ICs cruciais
- Exibir status do IC

- Ocultar ou revelar um IC no layout do Visualizer
- Segurança de dados com base em funções.
- Executar MDRs externos
- Obter ajuda online para os recursos do Visualizer

Mais informações:

Realizar análise da causa raiz (na página 593)
Administração do Visualizer (na página 593)

Realizar análise da causa raiz

Usando Visualizer com Visualizador do CMDBf, é possível realizar uma análise de causa raiz.

Para realizar uma análise de causa raiz

1. No Visualizer, localiza um IC de serviço em uma condição de problema em particular (por exemplo, lento ou indisponível).
2. Clique com o botão direito do mouse no IC e selecione Criar IC de foco.
3. Selecione um filtro de Causa raiz usando os seguintes critérios:
   - Tipo de classe: não aplicável
   - Dependendo do relacionamento do fornecedor: todos os relacionamentos a serem exibidos para análise de causa raiz.
4. Clique em Exibir.

   No gráfico resultante, todos os ICs que estão relacionados ao IC focal são exibidos como especificados nos filtros. Todos os caminhos entre os ICs incluem ICs intermediários para o nível padrão.
5. Navegue para os ICs e os inspecione quanto a incidentes, problemas ou mudanças recentes como candidatos para a causa raiz da condição do IC focal.
6. Ativar o CA CMDB em contexto para um IC em particular.
7. Clique no Visualizador do CMDBf.

   Uma Federated View é exibida com a lista de fornecedores do MDR para o IC.
8. Clique em Recuperar para obter os últimos atributos do MDR.

   Os atributos do MDR são atualizados.

Administração do Visualizer

A interface de administração do Visualizer pode ser usada para editar as configurações do CMDB Visualizer. Estas funções estão disponíveis apenas para funções com privilégios de administrador.

A interface de administração do Visualizer oferece as seguintes guias:

Guia Configuração do Visualizer

Permite configurar as informações do servidor e de exibição de ICs.

Guia Tipo de relacionamento

Define as características gráficas dos relacionamentos.

Observação: essa página é desativada em um servidor secundário do Visualizer.

Guia Status do IC

Define as características gráficas de ICs.

Observação: essa página é desativada em um servidor secundário do Visualizer.

Guia Filtros

Cria, edita e exclui os filtros para análise de ICs.

Observação: essa página é desativada em um servidor secundário do Visualizer.

Guia Pós-configuração de ícone

Mapeia uma família de IC para a sua respectiva imagem de ícone quando o CMDB Visualizer tiver sido atualizado de r11.2 para Release 12.7.

Observação: para obter mais informações sobre definições do Visualizer, consulte a ajuda online do CMDB Visualizer.

Adicionar um ativo detectado

É possível alterar ativos não proprietários no Management Database (MDB) para itens de configuração proprietários.

Para adicionar um ativo detectado

1. Clique no botão Ativos detectados na página Lista de itens de configuração.

   A página Pesquisa de ativo descoberto aparece.

2. Clique em Pesquisar para exibir a Lista de ativos detectados.
3. Selecione na lista o ativo que deseja adicionar como item de configuração, clique com o botão direito do mouse no ativo e selecione Criar novo item de configuração no menu pop-up exibido.

   A janela Criar novo item de configuração aparece com informações sobre o item preenchendo alguns dos campos.

4. Preencha todos os campos restantes aplicáveis ao novo item de configuração e clique em Continuar.

   Observação: apenas nome e classe são valores obrigatórios para a criação de um item de configuração.

5. Digite os dados necessários nos campos adequados na guia Atributos.

   A família da classe selecionada para o item de configuração determina os atributos que aparecem na guia. As informações digitadas aqui são determinadas pelos processos comerciais e pelas informações que deseja armazenar e exibir de um item de configuração.

6. Clique em Salvar.

   O ativo descoberto é adicionado.

Sinalizadores Ativo e IC

Dois sinalizadores de atributo comuns podem categorizar ainda mais o tipo de IC/ativo para fins de filtragem e controlar quais entidades são visíveis no CA SDM ou em outros produtos, como o CA APM.

Os sinalizadores são os seguintes:

IC? (SIM/NÃO)

Identifica itens de configuração.

Ativo? (SIM/NÃO)

Identifica ativos.

Por padrão, um IC criado pelo CA CMDB é sinalizado como um IC e não como um Ativo. É possível substituir isso, se necessário. Um IC também pode ser um ativo. O CA CMDB não permite que o sinalizador Ativo seja alterado assim que for definido para Sim. O sinalizador Ativo é normalmente definido para Sim quando um ativo é criado pelo CA APM.

Esses sinalizadores são exibidos em todos os formulários de detalhes do IC e no recurso de pesquisa do IC. Os valores podem ser atualizados no formulário de detalhes do IC, no GRLoader e nos serviços web do CA CMDB. O recurso Editar na lista também suporta atualizações de novos sinalizadores em vários registros.

O nome do atributo de objeto para o sinalizador de IC é **is_ci**. O nome do atributo de objeto para o sinalizador Ativo é **is_asset**. Estes nomes são atributos SREL que se referem a bool. Os nomes de atributo podem ser usados como marcas XML do GRLoader. Por exemplo, para alterar o valor padrão do sinalizador Ativo ao criar um IC com o GRLoader, adicione o seguinte XML para definir o novo IC:

```
<is_asset>SIM</is_asset>
```

CI Reconciliation

A reconciliação ajuda a garantir que as atualizações de várias origens de dados que se refiram ao mesmo objeto de negócios atualizem apenas um único IC, mesmo apresentando diferentes informações de identificação diferentes. *Ambiguidade* representa a possibilidade de um IC não ser único. Um IC pode ter possíveis "duplicatas" no CMDB, e as transações do IC podem ter mais de um IC de destino possível. ICs ambíguos poderão causar erros no CMDB, o que anula o seu valor e poderá levar a ações de negócios inadequadas.

A reconciliação automática de IC é uma importante vantagem do CA CMDB, que economiza um tempo significativo, comparada à manutenção de dados manual. O processo de reconciliação de ICs usa diversos atributos de identificação específicos. No entanto, a reconciliação automática pode causar os seguintes problemas:

- Correspondências falso-positivas

  Os ICs existentes são atualizados em vez de um IC ser criado.

- Correspondências falso-negativas

  São criados novos ICs em vez de um IC existente ser atualizado. O conjunto de ICs com atributos de identificação similares são ambíguos porque se assemelham ao mesmo objeto de negócios real com atributos de identificação similares.

O CA Service Desk Manager oferece suporte às seguintes abordagens de reconciliação:

Reconciliação com base em MDR (Passivo)

Permite que o CMDB reconcilie quaisquer dados ambíguos baseados no processo de Reconciliação com base em MDR.

Identificar e resolver ICs ambíguos (Reativo)

Identifica e resolve ICs ambíguos por meio da identificação e do gerenciamento de ICs existentes no CMDB.

Verificar e modificar dados de entrada usando uma área de trabalho de transação (Proativo)

Verifica e modifica dados de entrada antes de carregá-los no CMDB, usando uma TWA.

Mais informações:

Reconciliação com base em MDR (na página 598)
Como identificar e resolver ICs ambíguos (na página 600)
Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614)

Reconciliação com base em MDR

Reconciliação com base em MDR é feita no repositório de dados de gerenciamento, a fim de reduzir ainda mais a ocorrência de vários ICs no MDB que se refiram ao mesmo objeto no mundo físico.

Reconciliação com base em MDR trata o MDR como uma origem confiável que sempre usa a mesma ID de ativo federado ao comunicar informações sobre um único IC. Todas as atualizações de um dado MDR para uma determinada ID de ativo federado sempre atualizam o mesmo IC, mesmo ao identificar atributos alterados.

A reconciliação com base em MDR, o gerenciamento de reconciliação e a TWA (Transaction Work Area - Área de Trabalho de Transação) descritas nestas seções permitem controlar o processo de reconciliação. No entanto, para usar gerenciamento de reconciliação e a TWA com sucesso, primeiro, entenda como o CA SDM usa atributos de reconciliação.

Importante: Se você reinstalar ou reinicializar qualquer provedor de dados externo (por exemplo, CA Cohesion ACM),desative e reative sua definição de MDR no CMDB. Se o MDR reusar suas IDs de ativos federados, poderá ocorrer sobreposição inadvertida de dados de IC.

Mais informações:

Como a Reconciliação do MDR corresponde aos ICs (na página 599)
Como a Reconciliação do MDR identifica os ICs (na página 599)

Como a Reconciliação do MDR corresponde aos ICs

A reconciliação com base em MDR usa o seguinte processo para identificar o IC correspondente adequado:

1. Se a transação identificar uma ID, o IC será identificado, e a reconciliação, concluída.
2. Se a transação não especificar uma ID, o CA SDM verifica se os atributos de identificação agrupados são especificados e se correspondem a um IC. Se houver correspondência, a transação fará a reconciliação com o IC correspondente.
3. Se a transação não especificar uma ID ou atributos de identificação agrupados, a transação de IC usará os atributos de identificação (na página 599), conforme listados na seção abaixo.

Como a Reconciliação do MDR identifica os ICs

Reconciliação com base em MDR usa a seguinte precedência para identificar um IC:

1. ID (se uma transação especificar uma ID, a reconciliação será feita com êxito)
2. Atributos de identificação agrupados
   - ID do ativo agrupado
   - Nome do MDR
   - Classe do MDR
3. Atributos de identificação do IC
   - Inquilino (se a multilocação estiver instalada)
   - Nome
   - Número de série
   - Endereço MAC
   - Nome do sistema
   - ID do ativo alternativo
   - Nome do DNS

Como identificar e resolver ICs ambíguos

Recomendamos gerenciar ambiguidade em um IC por base de IC. Em cada caso, o Administrador de configuração deve detectar quando a ambiguidade existe e determinar a abordagem ideal. O CA SDM tem uma abordagem ampla para identificar e gerenciar ICs ambíguos que já estejam no CMDB.

O *índice de ambiguidade* é uma medida operacional da potencial não exclusividade de um item de configuração (IC) com base em seus atributos de identificação. O índice de ambiguidade pode medir a probabilidade de ICs "duplicados" no CMDB, ou a probabilidade de uma transação ter múltiplos destinos de IC.

Importante: Se você excluir manualmente os CIs com as consultas de banco de dados, pode haver erros relacionados aos índices de ambiguidade dos ICs. Para evitar esses erros, execute o utilitário cmdb_update_ambiguity e defina o parâmetro -full para 1. Esse parâmetro ajuda a garantir que você receberá índices de ambiguidade precisos ao executar o cmdb_update_ambiguity.bat ou o shell script.

Use o seguinte processo para identificar e resolver ICs ambíguos:

1. Identifique ICs ambíguos.
   - Calcule o índice de ambiguidade para todos os ICs
   - Verifique a lista de ICs ambíguos a partir do Gerenciador de filas
2. Determine se os atributos de identificação para cada IC são válidos.
3. Resolva o IC ambíguo com uma das seguintes ações:
   - Modifique os atributos de identificação
   - Exclua um IC do gerenciamento de ambiguidade
   - Rejeite uma Atualização de IC, desativando o IC
   - Substitua um IC

Mais informações:

Exemplo de ambiguidade de IC (na página 601)
Como identificar ICs ambíguos e determinar se os seus atributos de identificação são válidos (na página 602)
Como resolver ICs ambíguos (na página 610)

Exemplo de ambiguidade de IC

Dados a partir de quatro origens de dados diferentes são carregados no CMDB. Cada origem de dados usa seu próprio subconjunto de características de identificação. Por causa dessa inconsistência, existem mais ICs no CMDB do que o desejado.

A seguir são fornecidos exemplos de ambiguidade de IC:

Exemplo: ICs ambíguos

Os quatro ICs abaixo residem no CMDB:

- Nome(Server1) Nome DNS(dns1) Número de série(serial1)
- Nome(Server1) Nome DNS(dns1)
- Nome(Server2) Nome DNS(dns1) Número de série(serial1)
- Nome(Server3) Endereço MAC(mac1)

Devido a características de identificação compartilhadas, as duas instâncias do Server1 e Server2 são ambíguas entre si. O Server3 não é ambíguo.

Cada IC tem um índice de ambiguidade associado a ele. O índice de ambiguidade é aproximadamente o número de ICs existentes que correspondem a qualquer um dos atributos de identificação. Quanto maior o índice, maior o número de ICs que correspondem aos identificadores e, portanto, maior é a probabilidade de que os dados de IC foram inseridos de forma inconsistente e de que ICs adicionais foram criados de forma incorreta. ICs com um índice de ambiguidade igual a zero são exclusivos em todos os identificadores e, portanto, são não ambíguos.

O índice de ambiguidade de cada um dos ICs anteriores é

- Primeira instância para Server1: Contagem do nome correspondente de outros ICs + dnsname + número de série = 1+2+ 1=4
- Segunda instância do Server1:Contagem do nome correspondente de outros ICs + dnsname = 1+2 = 3
- Server2: Contagem do nome correspondente de outros ICs + dnsname + número de série = 0+2+ 1=3
- Server3: Contagem do nome correspondente de outros ICs + endereço mac = 0+0 = 0

Mais informações:

Como calcular o índice de ambiguidade (na página 603)
Exibir ICs ambíguos a partir da guia Administração (na página 608)
Exibir ICs ambíguos a partir do Gerenciador de filas (na página 609)

Como identificar ICs ambíguos e determinar se os seus atributos de identificação são válidos

Investigue qualquer IC com um índice de ambiguidade diferente de zero para determinar se ele é singular ou foi criado inadvertidamente por causa de reconciliação incorreta. Os ICs não são ambíguos por si mesmos, são ambíguos com outros ICs. Um sistema pode ter muitos conjuntos de ICs ambíguos, cada conjunto contendo ICs com valores comuns para atributos de identificação.

Quando pesquisar a ambiguidade de um IC, pesquise também a ambiguidade de outros ICs no mesmo conjunto. Ao resolver a ambiguidade de um único IC, você reduz ou elimina a ambiguidade de outros ICs nesse conjunto.

O CA SDM possui ferramentas de reconciliação que permitem encontrar ICs ambíguos e o conjunto de ICs do qual os ICs ambíguos são membros. É possível pesquisar a causa subjacente da ambiguidade e resolvê-la.

Ao gerenciar a ambiguidade, faça o seguinte:

1. Calcule o índice de ambiguidade para todos os ICs.
2. Use o gerenciador de filas para visualizar a lista de ICs ambíguos. O gerenciador de filas lista todos os ICs que forem ambíguos, em ordem descendente de ambiguidade.
3. Iniciando com o IC que possui o nível mais alto de ambiguidade no gerenciador de filas,
    a. Inspecione todos os ICs neste conjunto de ambiguidade. A guia de reconciliação no formulário de detalhe de IC de um único IC lista todos os outros ICs no conjunto de ambiguidade.
    b. Determine se todos os ICs no conjunto são legitimados ou se ocorreu um erro na reconciliação. Revise os atributos de identificação e determine se os IC no conjunto são criados corretamente ou se são criados devido a uma correspondência de reconciliação falso-negativa.
4. Determine quais ICs no conjunto, se houver, são falso-negativos.

Quando você tiver determinado que ocorreu uma correspondência de reconciliação falso-negativa, e foram criados ICs adicionais, determine qual IC é o válido e quais ICs foram criados incorretamente. Considere fatores, como atributos de identificação, e outros atributos, tais como data da última atualização, problemas relacionados, ocorrências e outros aspectos do IC.

Como calcular o índice de ambiguidade

Antes de ser possível iniciar o gerenciamento de ambiguidade, atualize o índice de ambiguidade dos ICs existentes e Transações de IC. Você atualiza o índice de ambiguidade para ICs e transações de IC executando o comando cmdb_update_ambiguity.

Importante: Execute o cmdb_update_ambiguity pelo menos uma vez para medir a ambiguidade do IC ou transação de IC. Se você não executar o comando, todos os índices de ambiguidade serão 0 (zero), o que implica em nenhuma ambiguidade.

Você pode executar o utilitário antes e durante o gerenciamento de ambiguidade. Programe o utilitário para ser executado periodicamente, de modo que os índices de ambiguidade reflitam o estado atual de seu sistema.

Para usar o índice de ambiguidade

1. Determine os parâmetros necessários para executar o utilitário.
2. Execute o utilitário.
3. Inicie o Cliente Web do CA SDM e navegue até as Listas de ICs ambíguos ou de transações de IC ambíguo para gerenciar a ambiguidade.

Mais informações:

Como identificar e resolver ICs ambíguos (na página 600)

Comando cmdb_update_ambiguity

Você pode calcular os índices de ambiguidade de IC e transação de IC inserindo a sintaxe de comando similar ao seguinte:

```
cmdb_update_ambiguity [parameters] –m { ci | twa | all }
```

Para parâmetros de comando, consulte Parâmetros cmdb_update_ambiguity (na página 606).

Por padrão, a verificação de IC é feita a partir da data da última verificação. Se for especificado "-full 1", é realizada uma verificação completa.

Exemplo: Calcule a ambiguidade de IC em um banco de dados do Microsoft SQL Server

O comando a seguir calcula o índice de ambiguidade para todos os ICs existentes e Transações na TWA:

```
cmdb_update_ambiguity –m all –d MSSQL –u servicedesk –p dbpassword -s dbserver1
```

Exemplo: Calcular a ambiguidade de IC em um banco de dados Oracle

O seguinte comando calcula o índice de ambiguidade de ICs e especifica informações de banco de dados.

```
cmdb_update_ambiguity –m ci –d Oracle –u mdbadmin –p dbpassword -s server1 -port 1521
–SID orcl
```

Como usar um arquivo de configuração

É possível especificar muitos parâmetros cmdb_update_ambiguity em um arquivo de configuração. É possível usar o arquivo de configuração para proteger configurações de parâmetro em um formulário criptografado usando ferramentas do sistema operacional. As palavras-chave e as respectivas opções de linha de comando são listadas na tabela parâmetro.

Observação: se especificar um parâmetro tanto na linha de comando como no arquivo de configuração, o valor da linha de comando substitui o valor no arquivo de configuração.

Exemplo: Use um arquivo de configuração para especificar os parâmetros de um banco de dados do Microsoft SQL Server

O comando a seguir executa o arquivo de configuração ambiguity_mssql.cfg.

```
cmdb_update_ambiguity –m all -c ambiguity_mssql.cfg
```

Formato do arquivo de configuração

As opções de arquivo de configuração são especificadas como *palavra-chave*=*valor*. No Windows, o separador de diretório pode ser uma barra invertida dupla (\\) ou uma barra simples (/). O nome do caminho não deve ser incluído nas aspas duplas ("").

As palavras-chave válidas e as correspondentes opções de linha de comando são listadas na tabela de parâmetro.

Observação: Uma marca hash (#) na coluna 1 inicia uma linha de comentário.

Exemplo: ajustes de configuração do Microsoft SQL Server

```
Arquivo de configuração #Sample do Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\\Program Files\\CA\\Service Desk Manager\\log
LogLevel=ERROR
SchemaName=dbo
```

Exemplo: Ajustes de configuração Oracle

```
Arquivo de configuração #Sample para Oracle
DBType=Oracle
DBUser=mdbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mdbadmin
```

Parâmetros cmdb_update_ambiguity

É possível especificar parâmetros na linha de comando ou em um arquivo de configuração (alguns parâmetros são apenas de linha de comando). Na linha de comando, use aspas ("") para incluir qualquer nome de caminho com espaços; no arquivo de configuração, não use aspas. Se algum parâmetro for especificado na linha de comando e também no arquivo de configuração, o valor da linha de comando substitui o valor do arquivo de configuração.

O comando cmdb_update_ambiguity usa os seguintes parâmetros:

Opção	Palavra-chave do arquivo de configuração	Valores	Observações
-m	(nenhum)	twa, ci, all	(Obrigatório) Apenas linha de comando twa = calcular ambiguidade somente em TWA. ci = calcular ambiguidade somente de ICs. all = calcular ambiguidade para ICs e TWA.
-d	DBType	MSSQL ou Oracle	(Obrigatório. Windows somente) Tipo de banco de dados Em Linux/UNIX, somente o Oracle é suportado e esta opção não é necessária.
-u	DBUser	<db user name>	(Obrigatório) Nome do usuário do banco de dados Um nome de usuário com espaços deve estar incluído em aspas (por exemplo: -u "sys as sysdba"). As aspas não são obrigatórias no arquivo de configuração.
-p	DBPassword	<db password>	(Obrigatório) Senha do usuário do banco de dados Uma senha com espaços deve ser incluída em aspas duplas (por exemplo: -p "secret code"). As aspas não são obrigatórias no arquivo de configuração.

-c	(nenhum)	<configuration file>	(Opcional) Apenas linha de comando Nome do caminho completo do arquivo de configuração. Deve estar incluído em aspas duplas se houver um espaço no nome do caminho.
-log	LogLocation	<directory to place log file>	(Opcional) Diretório do arquivo de log O diretório padrão é NX_ROOT\log.
-nível	LogLevel	INFO, ERROR, DEBUG	(Opcional) Nível de detalhe para gravar no arquivo de log. O valor padrão é ERROR.
-s	DBHost	<server name>	(Obrigatório) Nome de host do servidor do banco de dados. Para usar uma instância nomeada do Microsoft SQL Server, especifique *servidor**instância* na linha de comando, ou *servidor**instância* no arquivo de configuração.
-IC	IC	<CI uuid>	(Opcional) Calcular ambiguidade para o IC especificado e todos os ICs que forem ambíguos com ele.
-total	(nenhum)	0,1	(Opcional) Apenas linha de comando Otimiza o desempenho da verificação apenas considerando os ICs atualizados desde a última vez que o utilitário foi executado. Se definido em 1, induz uma verificação total de todos os ICs no cálculo do índice de ambiguidade. O padrão é 0. Este parâmetro não se aplica ao cálculo de ambiguidade da transação. O utilitário sempre avalia todas as transações na TWA.
-porta	DBPort	<port number>	(Obrigatório. Apenas Oracle) Número de porta Oracle
-SID	DBSID	<SID name>	(Obrigatório. Apenas Oracle) Nome SID Oracle

-h	(nenhum)		(Opcional) Imprime mensagem de uso de ajuda.
-esquema	SchemaName	<db schema name>	(Opcional) O padrão é mdbadmin para Oracle; ou dbo para Microsoft SQL Server.

Mais informações:

Comando cmdb_update_ambiguity (na página 603)

Exibir ICs ambíguos a partir da guia Administração

Após executar o utilitário cmdb_update_ambiguity, é possível exibir e gerenciar ICs ambíguos na guia Administração.

Para exibir ICs ambíguos, na guia Administração, vá para CA CMDB, Gerenciamento de reconciliação, ICs ambíguos.

A página Lista de ICs ambíguos exibe a lista de ICs ambíguos cujo índice é superior a 0 (zero).

Observação: ao clicar em Limpar filtro na página Lista de ICs ambíguos ou página Lista de transações de IC ambíguo, isso não elimina o campo Argumentos de pesquisa adicionais (ambiguidade > 0).

Mais informações:

Exibir ICs ambíguos a partir da guia Administração (na página 608)

Exibir ICs ambíguos a partir do Gerenciador de filas

Após executar o utilitário cmdb_update_ambiguity, é possível exibir e gerenciar ICs ambíguos a partir do Gerenciador de filas.

Para exibir ICs ambíguos a partir do Gerenciador de filas

1. Se você estiver no Gerenciador de filas do CA SDM, expanda a pasta do CMDB.
2. Vá para Gerenciamento de reconciliação, ICs ambíguos e clique em um dos seguintes itens:
   - Todas
   - Atualizado ontem
   - Atualizadas na semana passada
   - Atualizados no mês passado

   A lista de ICs ambíguos com índice maior que 0 (zero) é exibida.

   Observação: ao clicar em Limpar filtro na página Lista de ICs ambíguos ou página Lista de transações de IC ambíguo, isso não elimina o campo Argumentos de pesquisa adicionais (ambiguidade > 0).

Mais informações:

Como identificar e resolver ICs ambíguos (na página 600)

Como resolver ICs ambíguos

Após identificar ICs ambíguos e determinar se os seus atributos de identificação são válidos, resolva a ambiguidade entre os ICs no conjunto de ambiguidade usando uma ou mais das seguintes ações:

Modifique os atributos de identificação

Se você determinar que os atributos de identificação não estão completos ou são inválidos, defina os atributos de identificação de IC de modo que o IC seja único usando a interface web, GRLoader ou CMDBf.

Observação: quando o MDR atualizar o IC, o MDR pode desfazer as alterações de reconciliação que foram feitas manualmente.

Exclua um IC do gerenciamento de ambiguidade

Se você determinar que as características de identificação de ICs estão corretas e representam uma ambiguidade conhecida e válida, você pode remover o IC das listas de gerenciamento de ambiguidade e do cálculo de ambiguidade de outros ICs, e o IC pode ser marcado como não ambíguo (excluir ambiguidade).

Rejeite uma Atualização de IC, desativando o IC

Quando você determina que os atributos de identificação de um IC são incorretos e que atualizações usando esses atributos causam corrompimento de dados, o IC pode ser desativado, impedindo outras atualizações. O usuário ou MDR que gera as informações recebe um erro e a toda a transação é rejeitada.

Substitua um IC

Algumas vezes, as atualizações para o CMDB estão além do controle do administrador e os dados de identificação inválidos precisam estar no sistema com dados de atributo válido de não-identificação. Os dados de atributo de transação de entrada podem ser redirecionados de forma transparente a um IC substituto.

Observação: o redirecionamento transparente de dados de atributo de um IC para outro pode causar confusão, pois os dados de transação podem não estar armazenados no mesmo IC, como os atributos de identificação de transação levariam você a acreditar. Use este método com critério, quando os métodos anteriores não puderem ser usados.

Como excluir ICs do gerenciamento de ambiguidade

Algumas vezes você reconhece que, embora um IC em particular receba um índice de ambiguidade maior que zero, ele deve ser deixado assim como está. Qualquer IC com a caixa de seleção Excluir ambiguidade selecionada não é considerado parte do índice de ambiguidade ou dos recursos de gerenciamento de ambiguidade.

Excluir a ambiguidade para um IC

Você pode atualizar a opção Excluir ambiguidade para um IC a partir da interface da Web.

Para excluir a ambiguidade para um IC

1. Selecione o IC que deseja excluir do gerenciamento de ambiguidade na página Lista de ICs ambíguos.

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Selecione a caixa de seleção Excluir Ambiguidade na guia Reconciliação e clique em Salvar.

   O IC é excluído do cálculo do índice de ambiguidade e de outros recursos de gerenciamento de ambiguidade.

Como excluir ambiguidade usando o GRLoader

É possível atualizar a opção excluir ambiguidade para um IC usando o GRLoader, para definir o sinalizador not_ambiguous para o IC.

os valores not_ambiguous são os seguintes:

SIM (1)

Remove o IC do gerenciamento de ambiguidade. O IC é identificado como único independentemente dos atributos de identificação de outros ICs. O índice de ambiguidade do IC permanece zero.

NÃO (0) (padrão)

Esse IC é elegível para gerenciamento de ambiguidade. A singularidade dos atributos de identificação dos ICs determina o índice de ambiguidade desse IC. Os atributos de identificação desse IC são considerados ao avaliar o índice de ambiguidade de outros ICs.

Observação: para obter mais informações sobre o GRLoader, consulte a *Referência Técnica do CA CMDB*.

Como rejeitar atualizações

Quando um IC é marcado como Inativo, nenhuma atualização pode ser realizada nele. Defina o IC como Inativo se desejar que o CA CMDB rejeite os dados para um determinado IC (seja por nome, número de série, endereço MAC, e assim por diante) e deseja que MDR saiba da rejeição.

Dessa maneira, você pode rejeitar dados problemáticos imediatamente e refleti-los de volta à origem, onde o MDR pode corrigir a entrada rejeitada.

Para definir um IC como Inativo na interface da Web, edite o IC, defina-o como Inativo e clique em Salvar. Você também pode definir um IC como Inativo usando os serviços web do CMDBf ou o GRLoader. ICs inativos também podem ser reativados.

Substituir ICs ambíguos

É possível substituir um IC ambíguo para redirecionar dados a um IC de destino específico. É possível exibir ICs substituídos, que são Inativos e todas as atualizações de interface web são ignoradas para eles.

Observação: atualizações enviadas para ICs substituídos pelos serviços web CMDBf ou GRLoader são redirecionados para o IC que os substitui. No entanto, atualizações a atributos de identificação são ignoradas.

Para substituir um IC ambíguo:

1. Selecione o IC desejado para ser o IC focal (que substitui), na página Lista de ICs ambíguos.

   A página Detalhe de item de configuração aparece.

2. Clique em Editar.

   A página Atualizar item de configuração aparece.

3. Clique na guia Reconciliação.

   Todos os ICs que forem ambíguos com o IC focal são exibidos.

   Determine quais ICs você deseja substituir pelo IC focal. Inspecione todos os ICs na lista, clicando em cada um deles para executar sua página Detalhes do item de configuração.

4. Selecione um ou mais ICs ambíguos que deseja substituir pelo IC focal e clique em Substituir.

   O IC focal substitui os ICs selecionados.

Exibir ICs substituídos a partir da guia Administração

É possível exibir ICs substituídos a partir da guia Administração.

Para exibir ICs substituídos a partir da guia Administração, na guia Administração, vá para CA CMDB, Gerenciamento de reconciliação, ICs substituídos.

A lista ICs substituídos aparece.

Exibir ICs substituídos a partir do Gerenciador de filas

É possível exibir ICs substituídos a partir do Gerenciador de filas.

Para exibir ICs substituídos a partir do Gerenciador de filas:

1. Se você estiver no Gerenciador de filas do CA SDM, expanda a pasta do CMDB.
2. Expanda a pasta Gerenciamento de reconciliação
3. Clique no nó ICs substituídos.

   A lista ICs substituídos aparece.

Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação)

É possível armazenar temporariamente transações de IC e relacionamento antes da execução, copiando dados para a área de armazenamento temporário da TWA. Estando na área de armazenamento temporário, é possível manipular ICs e relacionamentos usando a interface web ou o SQL nativo.

Também é possível validar as transações de IC para evitar a criação de novos ICs quando você tiver que atualizar ICs existentes. Nesta abordagem, você exibe cada transação e os ICs potenciais que podem ser atualizados, de modo que possa reconciliar a transação manualmente com o IC de destino. Da mesma forma, transações de relacionamento podem ser validadas para fazer referência aos ICs corretos.

O *índice de ambiguidade* é uma medida operacional da potencial não exclusividade de um item de configuração (IC) com base em seus atributos de identificação. O índice de ambiguidade pode medir a probabilidade de ICs "duplicados" no CMDB, ou a probabilidade de uma transação ter múltiplos destinos de IC.

Verifique e modifique transações de IC ambíguas usando o seguinte processo:

1. Identifique transações de IC ambíguas.
   - Calcule o índice de ambiguidade para todas as transações de IC.
   - Verifique a lista de transações de IC ambíguas a partir do Gerenciador de filas
2. Determine se os atributos de identificação para cada transação de IC se ajustam ao IC desejado.
3. Resolva as transações de IC ambíguas com uma das seguintes ações:
   - Modifique os atributos de identificação
   - Especifique o IC de destino

Mais informações:

Exemplo de ambiguidade de transação de IC (na página 616)
Como identificar uma transação de IC ambíguo (na página 618)
Como resolver transações de IC ambíguo (na página 619)
Gerenciar Transações armazenadas temporariamente (na página 620)
Área de trabalho de transação (na página 621)
Preenchendo a área de trabalho de transação (na página 623)
Como usar a interface da Web para atualizar dados na TWA (na página 636)
Reconciliação manual (na página 638)
Como carregar transações para o CMDB (na página 641)
Administração da TWA (na página 643)

Exemplo de ambiguidade de transação de IC

Dados de transação a partir de diferentes origens de dados são carregados no CA CMDB. Cada origem de dados usa seu próprio subconjunto de características de identificação e pode não identificar por completo os ICs de destino para as transações. Por causa dessa inconsistência, podem existir mais Transações de IC no CA CMDB do que são válidas.

A seguir, está um exemplo de ambiguidade de transação de IC:

Exemplo: Transações de IC ambíguas

A seguinte transação de IC reside na TWA:

- Nome(Server1) Nome DNS(dns1), Número de série(serial1)

Os seguintes ICs residem no CA CMDB:

- Nome(Server2) Nome DNS(dns1)
- Nome(Server3) Nome DNS(dns1), Número de série(serial1)
- Nome(Server4) Endereço MAC(mac1), Número de série(serial1)

Devido a características de identificação compartilhadas, a transação do Server1 é ambígua com Server2, Server3, e Server4 no CA CMDB.

Cada transação de IC tem um índice de ambiguidade associado a ela. O índice de ambiguidade é aproximadamente o número de ICs existentes que correspondem a qualquer atributo de identificação, menos um, especificado na transação de IC. Quanto maior for o índice, maior é o número de outros ICs que correspondam aos identificadores de transação e, portanto, maior é a probabilidade de que dados de IC foram inseridos de forma inconsistente, e maior a possibilidade de que ICs adicionais foram criados de forma incorreta. Transações de IC com um índice de ambiguidade igual a zero têm atributos de identificação exclusivos em todos os ICs ou têm um IC de destino especificado e, portanto, são não ambíguas.

Exemplo: calcular o índice de ambiguidade

As seguintes transações de IC residem na TWA:

- Nome(Server1) Nome DNS(dns1), Número de série(serial1)
- Nome(Server2) Nome DNS(dns1), Número de série(serial1)

Os seguintes ICs residem no CA CMDB:

- Nome(Server1) Nome DNS(dns1), Número de série(serial1)
- Nome(Server2) Nome DNS(dns1), Número de série(serial1), Endereço MAC(mac1)

A primeira ambiguidade de transação (Server1) é 0, pois há uma correspondência exata com os atributos de identificação de ICs do Server1. O único IC de destino possível para essa transação é o IC do Server1.

A segunda transação (Server2) é ambígua com o IC do Server1 e o IC do Server2.

O índice de ambiguidade para a transação do Server2 consiste nos seguintes componentes:

- Número de ICs correspondentes com Nome (Server2) = 1
- Número de ICs correspondentes com Nome DNS (dns1) = 2
- Número de ICs correspondentes com Número de série (serial1) = 2

Com base nas características de identificação de IC compartilhadas, o índice de ambiguidade para a transação do server2 é (1-1) + (2-1) + (2-1) = 2

Como identificar uma transação de IC ambíguo

Verifique e modifique transações que têm ICs de destino ambíguos antes de carregar os dados da transação. Você também pode solucionar transações de IC que não possuem um IC de destino, mas que possuem atributos de identificação para um ou mais ICs existentes. Essa etapa de resolução verifica se o IC adequado é atualizado e evita que dados incorretos ou inconsistentes sejam criados.

A guia Reconciliação na página CI Transaction Detail lista todos os ICs que são ambíguos com esta transação de IC focal. Inspecione os atributos de IC, tais como data da última atualização, problemas relacionados, ocorrências e outros aspectos do IC, para identificar o IC de destino que corresponda à transação.

Observação: para exibir ambiguidade tanto para ICs quanto para transações de IC, você deve calcular o índice de ambiguidade usando o utilitário cmdb_update_ambiguity (na página 603).

Para obter mais informações, consulte Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614).

Exibir transações ambíguas a partir da guia Administração

É possível exibir e gerenciar transações ambíguas a partir da guia Administração.

Para exibir transações ambíguas, na guia Administração, vá para CA CMDB, Gerenciamento de reconciliação, Transações de IC ambíguo.

A lista de transações de IC que têm um índice superior a 0 (zero) é exibida.

Observação: ao clicar em Limpar filtro na página Lista de ICs ambíguos ou página Lista de transações de IC ambíguo, isso não elimina o campo Argumentos de pesquisa adicionais (ambiguidade > 0).

Exibir transações ambíguas a partir do Gerenciador de filas

É possível exibir e gerenciar transações ambíguas a partir do Gerenciador de filas.

Para exibir transações ambíguas a partir do Gerenciador de filas:

1. Se você estiver no Gerenciador de filas do CA SDM, expanda a pasta do CMDB.
2. Vá para Gerenciamento de reconciliação, Transações de IC ambíguo e clique em um dos seguintes itens:
   - Todas
   - Atualizado ontem
   - Atualizadas na semana passada
   - Atualizados no mês passado

   A lista de transações de IC que têm um índice de ambiguidade superior a 0 (zero) é exibida.

   Observação: ao clicar em Limpar filtro na página Lista de ICs ambíguos ou página Lista de transações de IC ambíguo, isso não elimina o campo Argumentos de pesquisa adicionais (ambiguidade > 0).

Como resolver transações de IC ambíguo

Após identificar transações de IC ambíguo e determinar se os atributos de identificação ou o IC de destino são válidos, resolva a ambiguidade entre a transação IC usando uma das seguintes ações:

Modifique os atributos de identificação

Se você determinar que os atributos de identificação não estão completos ou são inválidos, pode definir os atributos de identificação de IC de modo que o ele seja único usando a interface da Web.

Especifique o IC de destino

Se você determinar que o IC de destino não está definido ou não é válido, é possível especificar um IC para uma transação ambígua, de modo que os seus dados sejam direcionados a um IC de destino específico, independente dos valores dos atributos de identificação especificados na transação.

Especificar um IC de destino para uma Transação de IC ambíguo.

É possível especificar um IC para uma transação ambígua, de modo que seus dados sejam direcionados a um IC de destino específico, independentemente dos valores dos atributos de identificação especificados na transação.

Para especificar o IC de destino para uma Transação de IC ambíguo.

1. Selecione uma transação de IC na página Lista de transações ambíguas.

   A página Detalhes da transação do item de configuração aparece.

2. Clique em Editar.

   A página Atualizar transação de item de configuração aparece.

3. Na guia Reconciliação, selecione um IC na lista para designar o IC como o IC de destino para a transação. Clique em Set Target e, em seguida, clique em Salvar.

   O IC selecionado se torna o IC de destino da transação.

Gerenciar Transações armazenadas temporariamente

O CA CMDB fornece um recurso no qual é possível armazenar dados antes de carregá-los no CA CMDB. Esses dados "armazenados temporariamente" são guardados como transações na TWA. Uma transação armazenada temporariamente é uma unidade de trabalho que cria ou atualiza um IC ou Relacionamento. A TWA pode conter muitas transações para um determinado IC ou relacionamento.

É possível capturar dados que são carregados no CMDB antes que os dados estejam comprometidos, de modo que seja possível modificar:

- Dados não padrão podem ser organizados e padronizados
- Dados incompletos podem ser complementados. Por exemplo, é possível definir o local como "Nova York" para os nomes de ICs que se iniciem com "NY".
- É possível modificar dados que não correspondam às tabelas de pesquisa existentes (SRELs).
- As transações podem ser programadas para futura implementação.

- Faça a reconciliação de transações para os ICs existentes no CA CMDB antes de carregar os dados.
- Valide as transações de IC e de relacionamento para impedir a criação de dados inválidos ou novos ICs quando ICs únicos ou existentes tiverem que ser atualizados. Exiba cada transação e os ICs potenciais que podem ser atualizados, de modo que possa reconciliar a transação manualmente para o IC de destino.

É possível usar a TWA para ajudá-lo a gerenciar de maneira proativa o processo de reconciliação. Você pode configurar o GRLoader para carregar os dados para a TWA, em que o CA CMDB permite que você modifique os dados da transação para controlar transações que possam criar, atualizar potencialmente ou fazer referência ao IC errado.

Para obter mais informações, consulte Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614).

Área de trabalho de transação

O CA SDM fornece a TWA para inspeção e modificação de IC e dados de relacionamento antes de carregar os dados no CMDB.

O processo da TWA funciona da seguinte maneira:

1. Carregue os dados (na página 623) na TWA. O conteúdo pode incluir transações de ICs ou transações de relacionamento. O processo de entrada não tenta reconciliar os registros. Ele apenas preenche a área de trabalho com os registros de transações de ICs e de relacionamentos em uma das seguintes formas:
   - GRLoader – Lê dados XML e os armazena na TWA usando as opções -lttwa ou -lttwar.
   - SQL nativo – os dados são colocados na TWA usando o processamento de SQL padrão.
   - Cria uma transação de IC ou transação de relacionamento usando a interface da Web.

2. (Opcional) Faça a reconciliação manual de transações com os ICs existentes no CMDB antes de carregar os dados. Você também pode simular o carregamento de dados (na página 629) para predeterminar se um conjunto de transações pode criar novos ICs (e, portanto, criar novas ambiguidades para outros ICs) ou relacionamentos.

   Para obter mais informações, consulte Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614).

3. Modifique os dados. É possível modificar a TWA a partir das seguintes origens:

   interface de usuário do CA SDM

   A interface de usuário baseada em web permite exibir e modificar transações na área de trabalho.

   SQL nativo

   Ao efetuar muitas mudanças em várias transações, o SQL nativo pode modificar os dados na TWA.

   Observação: as alterações feitas usando SQL nativo podem ignorar toda a segurança do CA SDM.

4. O GRLoader carrega os dados da TWA para o CA CMDB usando as opções -lftwa ou -lftwai. Cada linha da TWA é tratada como uma transação separada.

   1. Se ocorrer algum erro após uma execução do GRLoader, o código de erro é adicionado à transação para indicar que ela está incompleta (a fim de facilitar futuras tentativas).
   2. Todos os outros registros são identificados como transações concluídas.

5. Revise os resultados da transação e corrija quaisquer erros usando a interface da Web. Repita as etapas 3 e 4 conforme necessário.

   Observe o seguinte:

   - Se você criou quaisquer famílias ou atributos personalizados e quer que suas colunas apareçam na área de trabalho, modifique a área de trabalho para incluir as colunas personalizadas. Para obter mais informações, consulte Ampliar o objeto TWA (na página 643).
   - Use a última versão do GRLoader para tirar vantagem da TWA. Se você estiver usando um produto que inclui uma release anterior do GRLoader, atualize-a para a versão mais recente.
   - As alterações feitas às transações na TWA não são auditadas.

Preenchendo a área de trabalho de transação

Se você é responsável por preencher a área de trabalho de transação, recomendamos entrar em contato com o CA Services para obter assistência com este processo.

Dados inseridos podem vir de diversas origens, incluindo:

- Produtos da CA, como o CA Cohesion ACM e o CA Spectrum, que importam dados usando o GRLoader
- Qualquer outro MDR que importe dados usando o GRLoader
- CA CMDB (em produção)
- Planilhas do Microsoft Excel
- Tabelas de banco de dados
- Uma ferramenta de ETL escolhida por um fornecedor

Consulte Limitações do banco de dados (na página 647) para obter mais informações.

Como carregar dados na TWA usando o GRLoader

As seguintes opções do GRLoader oferecem suporte aos usos da TWA:

-lttwa

Carrega dados XML para a TWA no estado inicial.

-lttwar

Carrega dados XML para a TWA no estado pronto.

-lftwa

Carrega transações ao CMDB a partir da TWA.

-lftwai

Carrega transações ao CMDB da TWA e desativa transações bem-sucedidas.

Os documentos XML de entrada do GRLoader podem ser carregados no CMDB ou na TWA sem modificação.

O carregamento de dados na área de trabalho de transação pode ser feito usando o GRLoader com a opção –lttwa (carregar na TWA). No arquivo de configuração do GRLoader:

```
grloader.loadtotwa=yes
```

No modo TWA, em vez de criar ICs e relacionamentos de forma direta, o GRLoader insere as informações nas tabelas da área de trabalho de transação. Depois de carregados na TWA, os dados podem ser editados, alterados e verificados. Concluído o processo de modificação de dados, é possível carregar transações individuais no CMDB usando –lftwa ou -lftwai.

Ao carregar dados de IC no CMDB, os ICs são submetidos à reconciliação automática, a qual, se for bem-sucedida, fará com que os dados de um único objeto de negócios atualizem um único IC no CMDB. Ao carregar *transações de ICs* no TWA, não ocorre nenhuma reconciliação automática. Múltiplas transações com atributos de identificação destinadas a um único IC podem aparecer na TWA. As linhas existentes na TWA não são atualizadas quando novas linhas são adicionadas no modo carregar para a TWA mesmo se forem uma correspondência perfeita de um IC existente. Mesmo definições idênticas de IC podem aparecer várias vezes na TWA.

O GRLoader valida os valores de dados ao executar no modo de carregamento da TWA (-lftwa ou -lftwai) para criar objetos no CMDB ou ao executar usando o modo de simulação (-simci ou –simrel). Consulte Como simular operações da TWA (na página 629) para obter mais detalhes. Os valores de dados não são validados quando o GRLoader estiver executando no modo de carregamento para TWA (-lttwa ou -lttwar).

O parâmetro -lttwai (ou opção de configuração grloader.loadtotwa.inactivate) desativa transações da TWA carregadas com sucesso. Após uma transação carregada com sucesso ter sido marcada como inativa, ela pode ser permanentemente eliminada da TWA usando Arquivamento/eliminação.

Exemplo: Carregar no CMDB

O seguinte comando carrega dados diretamente no CMDB:

```
grloader … -i mydata.xml –a –n
```

O arquivo XML mydata.xml contém:

```
<GRLoader>
  <ci>
     <name>server1</name>
     <class>Server</name>
   </ci>
</GRLoader>
```

Exemplo: Carregar na TWA

O seguinte comando carrega os dados na TWA, de forma que possam ser manipulados antes de carregá-los no CMDB:

```
grloader … -i mydata.xml -lttwa
```

Mais informações:

Entrada XML (na página 625)
Pesquisa (na página 626)
Formato da data (na página 627)
EMPTY (na página 628)

Entrada XML

O GRLoader usa os dados da entrada XML. Ao carregar dados na TWA, as seguintes colunas XML são mapeadas para evitar conflitos quando os nomes das colunas se sobrepõem aos nomes padrão no banco de dados.

DO nome XML	PARA a coluna do banco de dados
inquilino	tgt_tenant
id	tgt_id
delete_flag	tgt_delete_flag

Para relacionamentos, é aplicado o seguinte mapeamento:

DO nome XML	PARA a coluna do banco de dados
name	provider_name ou dependent_name
dns_name	provider_dns_name ou dependent_dns_name
delete_flag	tgt_delete_flag

Os mapeamentos são revertidos ao carregar as tabelas de banco de dados da TWA.

Pesquisa

Ao especificar dados para atributos de pesquisa (SREL), na TWA, eles devem ter o mesmo formato que se especificados no CML nativo para o GRLoader. Os atributos de pesquisa aceitam apenas um conjunto específico de valores que devem ser definidos em tabelas relacionadas no CA SDM. Tais atributos também podem ter restrições e exceções adicionais que devem ser atendidas para que a atribuição ocorra. Os valores especificados são os mesmos, independente de serem especificados usando interface da web XML, SQL, ou TWA.

Para determinar se um atributo é um SREL, consulte as seguintes seções *Referência técnica do CA CMDB* :

- Famílias e Classes (os atributos SREL são identificados)
- Contato e outros campos de pesquisa
- Campos validados com base em dados em tabelas existentes (SREL)

Exemplo: Pesquisar XML

No exemplo a seguir, a coluna SREL alternativa é determinada especificando o parâmetro de pesquisa:

```
<ci>
<name>server1</name>
<owner lookup="userid">mckpe99 </owner>
</ci>
```

Na TWA, é possível fazer o mesmo acrescentando o sufixo à coluna SREL alternativa com o valor de dados, entre delimitadores (consulte grloader.workarea.delimiters a seguir). Assim sendo, a transação equivalente está representada na área de trabalho de transação da seguinte forma:

ID	Nome	Proprietário
100	server1	mckpe99 {userid}

Você também pode definir o caractere usado acima no arquivo de configuração grloader:

```
grloader.workarea.delimiters=xy
```

x e y são caracteres diferentes que, em geral, não aparecem na área de trabalho.

Formato da data

O GRLoader oferece suporte às seguintes opções de formato de data em XML.

- datefmt=UTC
- datefmt=localtime (padrão)

Exemplos: datefmt XML

```
<ci>
<name>server1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>

<ci>
<name>server3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

Assim sendo, a transação equivalente está representada na área de trabalho de transação da seguinte forma:

ID	Nome	purchase_date
101	server1	1241197235
102	server2	2009/05/01

Observação: Se houver caracteres especiais, como, por exemplo, barra (/), o formato da data será "localtime". Observação: Se não houver caracteres especiais, o formato da data seguirá o horário UTC.

EMPTY

O GRLoader oferece suporte à opção update_if_null no XML que limpa um campo no CMDB. O exemplo a seguir limpa o campo do proprietário do server1. Sem esse atributo, o campo em questão não é afetado. Ao usar a TWA, é possível empregar a palavra-chave EMPTY.

Exemplo: XML update_if_null

```
<ci>
<name>server1</name>
<owner update_if_null="yes"></owner>
</ci>
```

Na TWA, o valor do banco de dados é zerado especificando a palavra-chave EMPTY como valor de sequência de caracteres. A transação equivalente na área de trabalho é a seguinte:

ID	Nome	Proprietário
102	server1	EMPTY

O valor da palavra-chave pode ser definido usando a opção de configuração grloader.emptyvalue:

```
grloader.emptyvalue=xxxx
```

xxxx representa qualquer sequência de caracteres que normalmente não aparece nos dados da área de trabalho.

Como simular Operações da TWA

Você pode predeterminar se um conjunto de transações pode criar novos ICs ou relacionamentos (e, portanto, criar novas ambiguidades para outros ICs) usando as seguintes opções:

–simci

Simula apenas o processamento de transações de IC. Pode ser usado para determinar se as transações criam ou atualizam ICs. Quando for usada a opção -simci, o GRLoader executa a validação de dados.

–simrel

Simula apenas o processamento de transações de relacionamento. Pode ser usado para determinar se as transações de relacionamento criam ou atualizam relacionamentos. A opção –simrel verifica relacionamentos quanto à existência dos ICs dependentes e provedor, valida tipos de relacionamento, e assim por diante.

A saída do modo de simulação é direcionada para a TWA ou para o arquivo _err.xml file. No modo de carregamento normal, o arquivo _err.xml contém a entrada de IC e um comentário indicando se o IC foi inserido ou atualizado. Quando a simulação for usada, a mensagem do GRLoader na Lista de transações do IC indica se o IC ou relacionamento foi inserido ou atualizado, com outras mensagens de erro relevantes. O estado da transação permanece inalterado.

A simulação também pode ser ativada em um arquivo de configuração usando as opções **grloader.simulateloadci** e **grloader.simulateloadrelation**.

Observação: se a entrada do GRLoader criar ICs e relacionamentos ao mesmo tempo, a opção –simrel pode processar somente ICs reais, não ICs programados para criação. Por causa dessa limitação, -simci e –simrel são mutuamente excludentes.

Como usar o SQL para atualizar dados na TWA

A TWA é armazenada no MDB e você pode atualizá-la diretamente com consultas SQL.

Mais informações:

Tabelas da TWA (na página 630)
Nomes de coluna SQL da TWA (na página 631)
Inserir novos registros na TWA (na página 633)
Como usar o driver ODBC (na página 634)
Identificadores de IC no TWA (na página 634)
Como definir status de transação (na página 635)
Como compartilhar tabelas com o CA SDM (na página 635)

Tabelas da TWA

As tabelas da área de trabalho de transação (TWA) incluem:

ci_twa_ci

Uma tabela exclusiva que contém todos os atributos de todas as famílias do IC. A tabela armazena dados em um formulário desnormalizado, a fim de permitir que os clientes e serviços entendam e manipulem o conteúdo.

ci_twa_relation

Complementa a tabela ci_twa_ci. Esta tabela contém informações de relacionamentos de ICs.

Os nomes das colunas da TWA correspondem aos atributos usados com o GRLoader, salvo algumas exceções.

Observação: para informações de atributo de IC, consulte a *Guia de Referência Técnicas do CA CMDB*.

Nomes de coluna SQL da TWA

Nomes de coluna nas tabelas ci_twa_ci e ci_twa_relation correspondem aos nomes de atributo de IC e Relacionamento com algumas exceções.

Campos da TWA comuns a ci_twa_ci e ci_twa_relation

apply_after_dt (Aplicar após a data)

O GRLoader somente executa a transação se a data atual estiver após o campo Aplicar após a data. Medido em segundos a partir da data. Se o valor for zero (0), este campo será ignorado.

tran_chg_ref_num (Requisição de mudança)

Especifica o identificador da requisição de mudança associado a essa transação. A opção –chg do GRLoader usa este atributo para selecionar somente as transações com o número de requisição de mudança específico.

Observação: para obter mais informações sobre o uso da opção –chg, consulte Filtrar por número de requisição de mudança (na página 643).

tran_status (Status da transação)

Especifica que o status da transação deve ser um dos seguintes valores (somente transações com tran_status=1 são executadas).

Valor	Descrição breve	Descrição longa
0	Inicial	Valor padrão: Requer intervenção a fim de alterar para "Pronto", de modo que o GRLoader processe essa transação
1	Pronto	A transação está pronta para ser carregada no IC apropriado ou nas tabelas de relacionamentos
2	Com êxito.	Transação processada com êxito
3	Aviso	Aviso emitido durante o carregamento no ca_owned_resource/bmhier
4	Erro	Erro detectado durante o carregamento no ca_owned_resource/bmhier
40000+	Somente para uso do cliente	

tran_message (Mensagem)

Mensagem do GRLoader que exibe os resultados do carregamento ou simulação.

tran_dt (Data da transação)

Evita a substituição acidental de informações atuais por dados de transação antigos. A data da transação é comparada com a data da última modificação do IC, e o GRLoader rejeita a transação se o IC for mais recente.

Se o GRLoader rejeitar uma transação como mais antiga do que o IC de destino, verifique se a transação ainda é aplicável e defina manualmente a data da transação como sendo mais atual e execute novamente o GRLoader.

tgt_delete_flag (Ativo?)

Desativa o IC ou relacionamento de destino. Defina esse valor para 1 (um). Não é o mesmo que definir delete_flag em 1, o que indica que a transação deve ser excluída.

colunas de ci_twa_ci

Além dos nomes de coluna abaixo, também é possível especificar nomes de atributo de IC como nomes de coluna em suas instruções de SQL.

tgt_id (IC de destino)

Especifica a UUID do IC de destino. Usado ao realizar reconciliação manual.

superseded_by (Substituído por)

Especifica a UUID do IC substituído.

tgt_tenant (Inquilino)

Especifica o nome do inquilino atribuído ao IC de destino. O inquilino somente poderá ser atribuído durante a criação do IC caso o usuário do GRLoader tenha autorização adequada. Aplica-se somente quando a multilocação é ativada.

colunas de ci_twa_relation

Além dos nomes de coluna abaixo, também é possível especificar nomes de atributo de relacionamento como nomes de coluna em suas instruções de SQL.

Use os seguintes nomes de coluna de banco de dados ao usar SQL para definir transações de relacionamento:

provider_name (Nome do provedor)

provider_mac_address (Endereço MAC do provedor)

provider_serial_number (Número de série do provedor)

provider_system_name (Nome de host do provedor)

provider_asset_num (Número de ativo do provedor)

provider_dns_name (Nome DNS do provedor)

provider_tenant (Inquilino provedor)

E

dependent_name (Nome dependente)

dependent _mac_address (Endereço MAC dependente)

dependent _serial_number (Número de série dependente)

dependent _system_name (Nome do host dependente)

dependent _asset_num (Número do ativo dependente)

dependent _dns_name (Nome do DNS dependente)

dependent_tenant (Inquilino dependente)

Se o provedor ou UUIDs de IC dependente forem conhecidos, é possível usar os seguintes campos:

O provider_id especifica a UUID do IC provedor

dependent_id especifica a UUID do IC dependente

Observação: provider_tenant e dependent_tenant só se aplicam quando a multilocação estiver ativada.

Inserir novos registros na TWA

É possível inserir um novo registro nas tabelas ci_twa_ci e ci_twa_relation externamente ao CA SDM.

Para inserir registros nas tabelas ci_twa_ci e ci_twa_relation, especifique 0 na coluna ID como:

```
insert into ci_twa_ci values(id, name) values(0,'test-ci');
insert into ci_twa_relation values(id, type) values(0,'test-relation-type');
```

Cuidado: se a multilocação estiver ativada, forneça o inquilino, os atributos tgt_tenant, provider_tenant ou dependent_tenant, conforme for apropriado. Se você criar transações da TWA sem inquilino especificado, será considerado o inquilino Público.

Como usar o driver ODBC

É possível usar SQL em vez do GRLoader para carregar a TWA. Recomendamos o uso do driver ODBC fornecido com o CA SDM, em vez de serviços SQL nativos. O uso do driver ODBC oferece os seguintes benefícios:

- Desempenho
- Segurança
- Independência de banco de dados
- Integridade de dados em um ambiente no qual poderá haver atualizações de banco de dados originárias do servidor do CA SDM ao mesmo tempo em que uma ferramenta de edição em massa é executada.

Cuidados

- Somente drivers ODBC do CA SDM honram recursos de segurança como multilocação, particionamento de dados e acesso de função. O SQL executado usando drivers DBMS nativos não reforça a segurança.
- Faça backups frequentes dos dados ao efetuar atualizações com SQL nativo.

Identificadores de IC no TWA

Na tabela ci_twa_ci, três identificadores estão associados a uma transação de IC: ID, tgt_id e superseded_by, Esses atributos são:

- ID é o número de sequência da transação. **Não modifique este campo.** As IDs de 1 a 2.000.000.000 são reservadas para uso dos sistemas que modificam a TWA fora do servidor do CA SDM. As IDs de 2.000.000.001 a aproximadamente 4 bilhões são reservadas para uso do CA SDM. Quando não houver mais IDs para uso dos sistemas, reinicie a tabela.
- tgt_id, provider_id, ou dependent_id são a UUID do IC de destino. Defina este campo sempre que você executar reconciliação manual.
- superseded_by é a UUID do IC substituto. Defina este campo sempre que atribuir manualmente o IC substituto para a transação.

Como definir status de transação

É possível definir o status (tran_status) de cada transação na TWA. Para que o GRLoader processe uma transação, o status deve ser definido como Pronto (tran_status=1).

Valor	Descrição breve	Descrição longa
0	Inicial	Valor padrão: Requer intervenção a fim de alterar para "Pronto" para que o GRLoader processe esta transação
1	Pronto	A transação está pronta para ser carregada no IC apropriado ou nas tabelas de relacionamentos
2	Com êxito.	Transação processada com êxito
3	Aviso	Aviso emitido durante o carregamento no ca_owned_resource/bmhier
4	Erro	Erro detectado durante o carregamento no ca_owned_resource/bmhier
40000+	Somente para uso do cliente	

Se a opção –lftwa do GRLoader for executada duas ou mais vezes, o status será atualizado após a primeira execução, e nenhuma das execuções subsequentes encontrará transações. Redefina o status das transações prontas antes de cada execução de –lftwa do GRLoader.

Para obter mais informações sobre como representar dados XML nas tabelas da TWA, consulte os exemplos de XML nas seções anteriores.

Como compartilhar tabelas com o CA SDM

Somente servidor SQL

Ao usar SQL para atualizar as tabelas ci_twa_ci e ci_twa_relation, defina a coluna last_mod_dt manualmente da seguinte maneira:

```
SET last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
```

Exemplo: definir last_mod_dt

O exemplo a seguir define o last_mod_dt:

```
UPDATE ci_twa_ci
        SET tran_status=1,
                last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
        WHERE tran_status=1
```

Observação: as atualizações da tabela TWA podem levar diversos minutos para aparecer na interface da Web ou no GRLoader. Para obter mais informações sobre o tempo de atualização, consulte a opção NX_DBMONITOR_TIMER_MINUTES.

Como usar a interface da Web para atualizar dados na TWA

É possível armazenar temporariamente transações de IC e de relacionamento antes da execução, copiando dados para a área de armazenamento temporário da TWA. Estando na área de armazenamento temporário, é possível manipular ICs e relacionamentos usando interfaces da Web.

Também é possível validar as transações de IC e de relacionamento para impedir a criação de dados inválidos ou novos ICs quando ICs únicos ou existentes tiverem que ser atualizados. Nesta abordagem, você exibe cada transação e os ICs potenciais que podem ser atualizados, de modo que possa reconciliar a transação manualmente com o IC de destino.

Para gerenciar a área de trabalho da transação, selecione a guia Administração e navegue para o CA CMDB, nó Área de trabalho de transação. A partir desse nó, é possível gerenciar as páginas da Área de Trabalho da Transação.

Observação: para obter mais informações, consulte a .*Ajuda online*.

Mais informações:

Gerenciar transações de IC (na página 637)
Gerenciar transações de IC ambíguas (na página 638)
Reconciliação manual (na página 638)

Gerenciar transações de IC

A página CI Transaction Detail exibe todos os atributos que não estiverem em branco na transação. Se você desmarcar a caixa de seleção Ocultar valores vazios, todos os atributos de IC serão exibidos. Para informações de atributo adicional, aponte para o nome do atributo.

É possível fazer o seguinte:

- Visualizar uma transação
- Criar uma transação
- Editar a transação.
- Salvar ou cancelar mudanças na transação (modo de edição).
- Redefinir os dados originais da transação (modo de edição).
- Exibir ou ocultar dados (guia Atributos)
- Definir o IC de destino (guia Reconciliação)

Após salvar uma única transação, clique na guia Reconciliação para que essa transação verifique se não há ambiguidade em seu IC de destino desejado. Se houver ambiguidade, será possível especificar um IC de destino (na página 620). Quando a entrada de todos os dados for concluída, é possível simular o carregamento de dados (na página 629) para validar os dados e verificar a reconciliação.

Importante: Os dados que você insere na TWA usando esta interface web devem seguir as regras descritas na seção "Como carregar dados na TWA usando o GRLoader (na página 623)".

A interface web do usuário não valida dados que diferenciam letras maiúsculas de minúsculas na TWA. Verifique se os dados inseridos correspondem exatamente aos valores de pesquisa. Alternativamente, ao executar o GRLoader, é possível especificar a opção -I para ativar pesquisas que não diferenciam letras maiúsculas de minúsculas.

Observação: mesmo se o tgt_id ou superseded_by estiverem armazenados como UUIDs na transação, eles serão exibidos como nomes de IC na interface da Web.

Gerenciar transações de IC ambíguas

Verifique e modifique transações que têm ICs de destino ambíguos antes de carregar os dados da transação. Você também pode solucionar transações de IC que não possuem um IC de destino, mas que possuem atributos de identificação para um ou mais ICs existentes. Essa resolução ajuda a garantir que o IC adequado seja atualizado e evita que dados incorretos ou inconsistentes sejam criados.

Após salvar uma única transação, clique na guia Reconciliação para que essa transação verifique se não há ambiguidade em seu IC de destino desejado. Se houver ambiguidade, será possível especificar um IC de destino (na página 620). Quando a entrada de todos os dados for concluída, é possível simular o carregamento de dados (na página 629) para validar os dados e verificar a reconciliação.

Para obter mais informações sobre reconciliação de dados na TWA, consulte Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614).

Reconciliação manual

Para reconciliar uma transação de IC manualmente, determine o IC de destino que corresponde aos atributos de identificação da transação e defina a tgt_id da transação como a UUID do IC de destino.

Ao processar uma transação que especifica uma tgt_id, o GRLoader atualiza o IC de destino com as informações da transação e o registra novamente se os atributos de identificação tiverem mudado.

É possível especificar o IC de destino, de forma explícita, na transação. Também é possível usar a guia Reconciliação para selecionar um IC de destino.

Para obter mais informações, consulte Verificar e modificar dados de entrada usando a TWA (Transaction Work Area - Área de trabalho de transação) (na página 614).

Especificar um IC de destino para uma Transação de IC ambíguo.

É possível especificar um IC para uma transação ambígua, de modo que seus dados sejam direcionados a um IC de destino específico, independentemente dos valores dos atributos de identificação especificados na transação.

Para especificar o IC de destino para uma Transação de IC ambíguo.

1. Selecione uma transação de IC na página Lista de transações ambíguas.

   A página Detalhes da transação do item de configuração aparece.

2. Clique em Editar.

   A página Atualizar transação de item de configuração aparece.

3. Na guia Reconciliação, selecione um IC na lista para designar o IC como o IC de destino para a transação. Clique em Set Target e, em seguida, clique em Salvar.

   O IC selecionado se torna o IC de destino da transação.

Gerenciar transações de relacionamento

A lista de transações de relacionamento exibe a entrada de dados de transações de relacionamento.

Usando essa página, você pode fazer o seguinte:

- Pesquisar transações de relacionamento.

Na lista, você pode fazer o seguinte:

- Criar uma transação de relacionamento
- Editar em lista (exceto para atributos de identificação)

Atualizar uma transação de relacionamento

É possível exibir e modificar dados para uma única transação de relacionamento. Na página Detalhes da transação do relacionamento, você pode fazer o seguinte:

- Criar uma transação de relacionamento
- Exibir a transação

- Editar a transação.
- Salvar ou cancelar mudanças na transação (modo de edição).
- Redefinir os dados originais da transação (modo de edição).

Para atualizar uma relação de relacionamento

1. Clique em Editar.

   A página Atualizar transação de relacionamento é exibida.

2. Modificar e preencher campos.
3. Selecione Ativo.
4. Clique em Salvar.

   A transação de relacionamento é salva.

Quando a entrada de todos os dados for concluída, é possível simular o carregamento de dados para validar os dados e verificar a reconciliação.

Importante: Os dados que você insere na TWA usando esta interface web devem seguir as regras descritas na seção "Como carregar dados na TWA usando o GRLoader (na página 623)".

A interface web do usuário não valida dados que diferenciam letras maiúsculas de minúsculas na TWA. Verifique se os dados inseridos correspondem exatamente aos valores de pesquisa. Alternativamente, ao executar o GRLoader, é possível especificar a opção -I para ativar pesquisas que não diferenciam letras maiúsculas de minúsculas.

Observação: mesmo se o provider_id ou dependent_id estiverem armazenados como UUIDs na transação, eles serão exibidos como nomes de IC na interface da Web.

Como carregar transações para o CMDB

Em vez de usar entrada XML para criar ICs e relacionamentos, você pode especificar as seguintes opções para selecionar a TWA como sua origem de entrada:

–lftwa (carregar da TWA)

–lftwai (carregar da TWA e desativar)

Observação: ao contrário dos outros modos do GRLoader que usam um arquivo err.xml, carregar da TWA retorna mensagens de erro para o campo Mensagem da transação para exibição.

À medida que as transações são processadas, o GRLoader define o status da transação para indicar êxito ou falha de cada transação da TWA. Se -lftwa do GRLoader for executada várias vezes consecutivas, defina o status da transação como Pronto entre as execuções do GRLoader, pois ele não tenta carregar dados que já estão carregados.

A transação é executada a partir da TWA como se o GRLoader estivesse executando usando a entrada XML. A segurança da transação baseia-se no usuário que carrega os dados da TWA, não no usuário que carregou a transação na TWA originalmente.

A auditoria é feita quando as transações são processadas com êxito.

Observação: antes de realizar o carregamento, você pode predeterminar se um conjunto de transações criará novos ICs ou relacionamentos usando as opções de simulação (-simci e -simrel). Consulte Como simular operações da TWA (na página 629) para obter mais informações.

Mais informações:

Como evitar a regressão de dados (na página 642)
Filtrar pelo número da requisição de mudança (na página 643)

Como evitar a regressão de dados

Embora os dados para um IC estejam na TWA, alguma outra ação pode atualizar esse IC no CMDB e fazer com que os dados de transação da TWA tornem-se inválidos. Para impedir regressão de dados indesejados, o GRLoader compara o campo da TWA tran_dt (Data da Transação) com o IC last_update_dt (Data da última modificação) ou relacionamento last_mod_dt (Data da última modificação). Se last_update_dt for mais recente, o GRLoader rejeita a transação da TWA e posta uma mensagem de erro para a coluna tran_message.

Você pode resolver essa situação fazendo um dos seguintes:

- Use a interface da Web para editar o IC ou o campo tran_dt (Data da transação) do relacionamento para um valor mais adequado.
- Defina a opção grloader.workarea.ignore_transaction_dates="yes" do GRLoader de forma que ele ignore as datas da transação e insira os dados.

Observação: se o GRLoader rejeitar uma transação que tenha a mesma data do IC de destino e, em seguida, você constatar que a transação deve ser executada, defina manualmente uma data mais atual para a transação e execute novamente o GRLoader.

Aviso. A opção ignore transaction dates pode causar a regressão dos dados. Ao atualizar um único IC ou relacionamento várias vezes na mesma execução de -lftwa do GRLoader, o last_update date do IC ou relacionamento é definido como o horário da primeira atualização. Para permitir várias atualizações do mesmo IC ou relacionamento, é feita uma verificação adicional para comprovar que o IC ou relacionamento foram atualizados após a inicialização do GRLoader. Se sim, a atualização é permitida.

Filtrar pelo número da requisição de mudança

A opção do -chg do GRLoader pode ser usada para selecionar somente transações associadas a um ticket de mudança. Para filtrar por número de mudança, é necessário definir o atributo da Requisição de mudança (tran_chg_ref_num) como o número de solicitação de mudança adequado.

Observação: a sequência de caracteres Requisição de mudança não é validada quando carregada no CMDB.

Exemplo: Filtrar por ticket de mudança

A seguinte opção carrega somente transações relacionadas à Requisição de mudança 23434.

```
grloader -lftwa -chg 23434
```

Administração da TWA

A TWA pode exigir a seguinte administração:

- Ampliar a TWA - obrigatório ao ampliar quaisquer famílias OOB ou ao definir suas próprias famílias personalizadas.
- Arquivamento e eliminação da TWA
- Como usar a TWA com o CA Cohesion ACM
- Limitações do banco de dados

Mais informações:

Ampliar o objeto TWA (na página 643)
Arquivamento e eliminação da TWA (na página 644)
Opções de comando do GRLoader da TWA (na página 645)
Opções do arquivo de configuração do GRLoader da TWA (na página 646)
Como usar o TWA com CA Cohesion ACM (na página 647)
Limitações do banco de dados (na página 647)

Ampliar o objeto TWA

Quaisquer modificações feitas no esquema de famílias do CA CMDB exigem mudanças no esquema da TWA. Se não houver famílias ou atributos personalizados definidos, a TWA não exigirá nenhuma modificação.

Para ampliar o objeto TWA

1. Personalize as famílias e atributos definidos pelo usuário usando os procedimentos em Extensão do CA CMDB no *Guia de Administração*.
2. Adicione os novos atributos de família ao esquema ci_twa_ci usando o criador de esquemas do Pintor de tela da web.

   Para adicionar um novo atributo ao esquema ci_twa_ci:

   1. Com o criador de esquemas do Pintro de tela da web, abra o esquema da tabela ci_twa_ci.
   2. Adicione a família desejada à tabela de extensão.
   3. Publique o esquema ci_twa_ci modificado.

   Observação: os novos atributos devem ser do tipo STRING e conter o valor de texto mais longo possível.
3. Adicione os metadados da família personalizada à TWA, conforme o seguinte procedimento:
   1. Com o Pintor de tela da web, abra o arquivo cmdb_metadata_site_families.htmpl.
   2. Adicione um PDM_INCLUDE para o arquivo cmdb_metadata_*extension*.htmpl apropriado, que foi criado para a família personalizada.

Arquivamento e eliminação da TWA

Para manter o TWA, o CA SDM fornece as seguintes regras de arquivo/eliminação:

Transações inativas de IC

Transações de IC de arquivos e eliminação que estão marcados para exclusão.

Transações bem-sucedidas de IC

Transações de IC de arquivos e eliminações que foram concluídos com êxito.

Transações inativas de relacionamento

Transações de arquivos e eliminação que estão marcados para exclusão.

Transações bem-sucedidas de relacionamento

Arquiva e elimina transações de relacionamento que foram concluídos com êxito.

É possível selecionar a frequência com que as regras são executadas ou se estão ativadas.

É possível personalizar e ativar as regras para habilitar o arquivamento e eliminação da TWA. Se você for um usuário intenso da TWA, esteja ciente das limitações do número de registros na TWA impostas pelo DBMS.

Se tiver que reinicializar a TWA para limpar todos os dados na TWA, faça o seguinte:

- Defina todas as transações como inativas
- Execute a eliminação de arquivo morto

Importante Não use o SQL para excluir todos os registros na TWA, pois ele exclui os registros de cabeçalho obrigatórios.

Opções de comando do GRLoader da TWA

O CA SDM fornece as seguintes opções de comando para uso no processamento da TWA do GRLoader:

-lttwa

Carrega XML no estado inicial.

-lttwar

Carrega XML no estado pronto.

-lftwa

Carrega transações da TWA

-lftwai

Carrega transações da TWA e desativa transações bem-sucedidas.

-chg *nnnn*

Usado com –lftwa e -lftwar. Carrega somente as transações associadas à requisição de mudança *nnnn*.

Observação: a sequência de caracteres Requisição de mudança não é validada quando carregada no CMDB.

-I

Ignore letras maiúsculas ou minúsculas de atributos de pesquisa. Por padrão, o texto em formato livre para atributos de pesquisa é processado como sensível a maiúsculas e minúsculas, exceto se esta opção for usada.

-simci

Determina se as transações de IC podem criar ou atualizar ICs. Quando essa opção for usada, o GRLoader realizará a verificação de erro apenas com relação a ICs.

-simrel

Determina se as transações de relacionamento podem criar ou atualizar relacionamentos. Essa opção verifica relacionamentos quanto à existência dos ICs provedores e dependentes, valida tipos de relacionamento e assim por diante.

Opções do arquivo de configuração do GRLoader da TWA

O CA CMDB fornece as seguintes opções da TWA para o arquivo de configuração do GRLoader:

grloader.emptyvalue=EMPTY

grloader.loadfromtwa=yes

grloader.loadfromtwa.inactivatesuccessful=yes/no

grloader.loadtotwa=yes

grloader.loadtotwa.ready=yes/no

grloader.workarea.delimiters={ }

grloader.workarea.ignore_transaction_dates=yes

grloader.simulateloadci=yes/no

grloader.simulateloadrelation=yes/no

Como usar o TWA com CA Cohesion ACM

Para usar a TWA com o processamento de ACM do CA Cohesion, aplique o patch RO08739 ao CA Cohesion ACM r5. Esse patch permite especificar a opção –lttwa no campo Outras opções, na guia Opções de exportação da definição de relatório de Exportação do CA CMDB. Atualize o componente GRLoader. Entre em contato com o suporte da CA em caso de dúvidas.

Limitações do banco de dados

A TWA está sujeita às seguintes limitações do banco de dados subjacente:

- Ao usar a TWA e o Microsoft SQL Server, o tamanho total de uma transação de dados não deverá exceder 8060 bytes.
- Ao usar os utilitários dbload e pdm_load, a operação de carregamento está restrita a 512 colunas.
- O Oracle tem uma limitação de 1000 colunas. Se você personalizar o CA CMDB, certifique-se de que o número total de atributos não exceda 1000 em todas as famílias (tanto as fornecidas pela CA quanto as definidas pelo usuário).
- As limitações do SQL Server 2005 são descritas na tabela a seguir.

Tipo de limitação	Limite (32 bits e 64 bits)
Colunas por tabela larga	30000
Colunas por tabela base	1024
Colunas por instrução SELECT	4096
Bytes por linha	8060
Linhas por tabela	Limitado pelo armazenamento disponível

Manutenção de dados do CA CMDB

As tarefas realizadas para manter os dados do CMDB exigem privilégios de administração. Essas tarefas incluem como configurar famílias, classes e tipos de relacionamento usados para gerenciar itens de configuração e informações de relacionamento.

Mais informações:

Estrutura de classe /família do CA CMDB (na página 648)
Alterar família/classe de um único IC (na página 649)
Alterar a família/classe de uma lista de ICs (na página 649)
Alterar a família/classe do IC usando o GRLoader (na página 650)
Extensão do CA CMDB (na página 650)

Estrutura de classe /família do CA CMDB

O CA CMDB fornece famílias de itens de configuração padrão e as classes de ICs que elas contêm.

Observação: para obter informações sobre a estrutura padrão de famílias/classes do CA CMDB, consulte a *Guia de Referência Técnica do CA CMDB*.

Observação: as famílias base a seguir do Service Desk e do CA APM não possuem suas próprias tabelas de extensão do CA CMDB:

- Computador
- Contato (como objeto base)
- Hardware
- Local (como objeto base)
- Organização (como objeto base)
- Outros
- Projeto
- Software

No CA CMDB, os ICs nessas famílias base recebem páginas Detalhes do IC com alguns campos irrelevantes e sem uma guia Atributos. Para aproveitar os recursos avançados do CA CMDB, como a capacidade de rastrear atributos específicos de famílias, controle de versão, instantâneos e linhas de base, recomendamos usar o recurso Alterar família e classe para converter esses ICs em famílias do CA CMDB.

Alterar família/classe de um único IC

É possível alterar a Família e a Classe de um único IC

Para alterar a Família e a Classe de um único IC

1. Selecione o IC que deseja alterar.
2. Clique em Editar.

   A página Atualizar item de configuração é exibida.
3. Altere o valor de Classe do IC. Selecionar a classe também determina a família do IC. É possível digitar um valor diretamente ou clicar na lupa para selecionar em uma lista de classes.
4. Clique em Salvar.

   A Família e a Classe do IC exclusivo são alteradas.

Alterar a família/classe de uma lista de ICs

É possível alterar a Família e a Classe de uma lista de ICs.

Para alterar a família/classe de uma lista de ICs

1. Na Lista de itens de configuração, clique em Mostrar filtro.
2. Preencha um ou mais campos Pesquisar para pesquisar os ICs que deseja editar.
3. Clique em Pesquisar.

   A Lista de itens de configuração é preenchida com todos os ICs que corresponderem aos critérios de pesquisa.
4. Clique em Editar na lista

   A Lista de itens de configuração exibe os campos que podem ser alterados para todos os ICs selecionados.
5. Edite os campos Família e Classe conforme desejado.
6. Clique em Alterar tudo.
7. Clique em Salvar.

   Ao atualizar a Lista de itens de configuração, ela exibe os ICs atualizados.

Alterar a família/classe do IC usando o GRLoader

É possível alterar a Família e a Classe de um único IC usando o GRLoader.

Para alterar a família ou a classe de um IC usando o GRLoader

1. Crie um código XML para alterar o atributo do IC.
2. Usando o GRLoader, abra o IC que deseja modificar.
3. Execute o XML por meio do GRLoader para alterar o atributo do IC.

   A Família e a Classe para um IC são alteradas.

Exemplo: definir a classe de um IC aberto como Documento

O exemplo a seguir mostra um fragmento de XML que define a classe de um IC aberto como *Documento*.

```
<ci>
    <name>documento número 1
    <class>Documento
</ci>
```

Importante: não tente atualizar os atributos Família e Classe de um IC ao mesmo tempo. Para alterar os dois, é necessário usar duas atualizações de IC separadas em duas chamadas separadas do GRLoader.

Extensão do CA CMDB

O CA CMDB é um sistema altamente flexível que pode ser estendido para incluir famílias, classes e atributos adicionais de acordo com as necessidades de sua organização. Novos atributos podem ser específicos às famílias ou *comuns* (aplicáveis a todas as famílias). Embora o CA CMDB forneça famílias predefinidas com muitas classes e atributos com base em padrões do setor, alguns casos de negócio exigem uma ou mais das seguintes atividades:

- Estender uma ou mais das famílias de IC adicionando novos atributos. Por exemplo, para adicionar uma coordenada de GPS a cada dispositivo na área de seu escritório, você pode definir um atributo gps_coordinate a ser adicionado a qualquer família desejada. Se você só deseja estender uma família, use o Designer de esquemas do Web Screen Painter para definir os novos atributos na tabela de extensão existente. Além disso, sempre que você adiciona um atributo, também deve modificar a página Detalhes, a guia Atributo e os formulários de metadados que usam o atributo. Para obter mais informações, consulte Adicionar atributos da família (na página 652).

- Estenda todas as famílias de IC adicionando um atributo comum. Para obter mais informações, consulte Adicionar atributos comuns (na página 653).
- Adicionar novas classes a uma família existente para suportar mais detalhes de classificação em seu sistema. Por exemplo, em vez da classe genérica Servidor, você pode criar uma classe distinta para cada modelo de dispositivo de servidor. Para obter mais informações, consulte Definir uma nova classe do IC (na página 654).
- Adicione uma nova família usando uma tabela de extensão existente e seus atributos. Uma nova família fornece uma maneira alternativa de organizar ou classificar ICs. Para obter mais informações, consulte Definir uma nova família do IC (na página 655).
- Se a classe existente ou a estrutura da família não corresponder a seus requisitos, você poderá recomeçar com um conjunto mínimo de atributos. Se você deseja adicionar uma nova família usando uma nova tabela de extensão, defina a nova tabela de extensão e seus atributos usando o Designer de esquemas do Web Screen Painter, além de criar os formulários necessários à exibição e atualização. Para obter mais informações, consulte Construção de uma nova estrutura de atributos (na página 656).

Importante: estender o CA CMDB exige conhecimento especializado das estruturas e tabelas de dados do CA SDM, além de familiaridade com o WSP (Web Screen Painter – Pintor de telas da web). Recomendamos que você entre em contato com Serviços da CA para obter ajuda nesta atividade e também que você leia e entenda completamente as seguintes seções antes de tentar estender as famílias e atributos do CA CMDB.

Adição de novos atributos do CA CMDB

Adicionar um novo atributo do CA CMDB exige um planejamento cuidadoso. O CA CMDB já fornece muitos atributos em suas famílias e classes predefinidas, assim, determine se eles são suficientes para suas necessidades antes de considerar a personalização.

Se você determinar que um novo atributo é necessário, recomendamos prosseguir de modo conservador, perguntando se você precisa:

- adicionar um ou mais atributos novos a uma família existente
- adicionar os novos atributos a mais de uma família

- adicionar um novo atributo comum, que se aplica a todas as famílias

Você pode estender uma família existente adicionando novos atributos. Por exemplo, se alguns dispositivos na área de seu escritório estiverem atribuídos a uma coordenada de GPS, você pode adicionar um atributo gps_coordinate a qualquer família de IC aplicável. Para obter mais informações, prossiga para Adicionar atributos da família (na página 652).

Depois que seus requisitos de atributo são identificados, se você determinar a necessidade de usar novas famílias e classes, consulte Adição de uma nova família ou classe do CA CMDB (na página 654).

Adicionar atributos da família

Você pode adicionar um novo atributo a uma ou mais famílias existentes usando o Designer de esquemas do Web Screen Painter, que atualiza o banco de dados para incluir o novo atributo e também atualiza as tabelas e arquivos associados do CA SDM. Este método tem preferência sobre atualizar as mudanças de tabelas e arquivos manualmente.

Para adicionar um novo atributo a uma família

1. Usando o Designer de esquemas do Web Screen Painter, abra o esquema que corresponde à tabela de extensão da família.
2. Adicione o atributo desejado à tabela de extensão.
3. Publique a tabela de extensão modificada.

Observação: GRLoader e Controle de versão automaticamente colhem novos atributos sem mais ação. No entanto, também recomendamos que a geração de log seja ativada. A geração de log é necessária para fins de auditoria; e Controle de versão ativado registrará todos os instantâneos.

Para ativar a geração de log, verifique se UI_INFO para o atributo está definido como **AUDITLOG**.

Depois que um novo atributo da família é criado, ele deve ser adicionado a cada formulário de exibição, de modo que os usuários possam exibir e atualizar esse atributo, e ao formulário de metadados específico à tabela de extensão. Para obter mais informações, vá para Adicionar atributos a formulários (na página 658).

Além disso, o Controle de versão exige metadados, inclusive informações sobre os cabeçalhos de coluna e os atributos de IC padrão relacionados. Você define novos metadados para todos os novos atributos que criar; para obter instruções, prossiga para Criar metadados (na página 659).

Adicionar atributos comuns

Atributos comuns são armazenados na tabela **ca_owned_resource** no objeto **nr**. Essa tabela fornece os seguintes campos personalizáveis:

- smag_1
- smag_2
- smag_3
- smag_4
- smag_5
- smag_6

Se você precisar de menos de sete atributos personalizados em todas as famílias de IC, esses campos fornecem uma solução prática.

Como fornecidos, esses campos personalizados não são exibidos em nenhum formulário. Para permitir que os usuários do CA CMDB exibam ou atualizem um campo smag_*n*, use o Web Screen Painter (WSP) para adicioná-lo a um formulário de exibição conforme desejado. Todas as funções de registro em log e do GRLoader já estão ativadas.

Observação: para procedimentos do Designer de esquemas do Web Screen Painter, consulte o capítulo "Personalização" do *Guia de Implementação do CA Service Desk* e a seção Personalizar o esquema do banco de dados da Ajuda online do Web Screen Painter.

Adição de uma nova família ou classe do CA CMDB

Adicionar uma nova família do CA CMDB exige um planejamento cuidadoso. O CA CMDB fornece muitas famílias e classes predefinidas, assim, determine se elas são suficientes para suas necessidades antes de considerar a personalização. Se não, alguns novos requisitos podem ser atendidos de uma das seguintes maneiras:

- definindo uma nova classe em uma família existente
- definindo uma nova família que usa uma tabela de extensão existente

Se você determinar que as tabelas de extensão existentes não são suficientes para suas necessidades, ignore esta seção e prossiga para a seção Construção de uma nova estrutura de atributos (na página 656) para criar uma tabela de extensão e os formulários de que ela precisa.

Definir uma nova classe de IC

Você pode adicionar novas classes para oferecer suporte a níveis mais altos de detalhamento de classificação. Por exemplo, em vez de usar uma das classes fornecidas pelo CA CMDB na família Hardware.Servidor, você pode definir classes adicionais para dispositivos de servidor diferentes.

Antes de criar uma nova classe de itens de configuração, determine se já existe uma classe adequada na Lista de classes do item de configuração.

Observação: se você também precisa de uma nova família para governar um novo conjunto de classes, ignore este tópico e prossiga para Definir uma nova família de IC (na página 655). Depois, você poderá retornar e preencher a nova família com classes.

Para definir uma classe de IC usando a interface de administração

1. Navegue até Lista de classes de itens de configuração.
2. Clique em Criar novo.

   A página Criar nova classe de item de configuração é exibida.
3. Digite um nome exclusivo para a nova classe.
4. Insira o nome da família apropriado no campo Família ou clique no ícone sobre o campo para pesquisar uma família.
5. Verifique se o campo Status do registro está definido como Ativo.
6. Clique em Salvar.

   A nova classe de IC é definida e está pronta para você criar novos ICs.

Definir uma nova família do IC

Antes de criar uma família de itens de configuração, determine se já não existe uma família adequada na Lista de famílias de itens de configuração. Se não houver, você pode criar novas famílias como um método alternativo de organizar ou classificar ICs usando atributos existentes.

Se a nova família de que você precisa não puder usar uma tabela de extensão existente (nem a tabela padrão), preencha todas as preparações adicionais descritas em Construção de uma nova estrutura de atributos (na página 656). A nova tabela de extensão pode ser usada para definir novas famílias.

Para definir uma família de IC usando a interface de administração

1. Navegue até Lista de famílias de itens de configuração.
2. Clique em Criar novo.

   A página Criar nova família de item de configuração é exibida.
3. Digite um nome exclusivo para a nova família.
4. Verifique se o campo Status do registro está definido como Ativo.
5. No campo Nome da extensão, selecione a tabela de extensão que identifica o tipo de família que você quer criar. Pode ser uma nova tabela de extensão que você criou recentemente.

   Por exemplo, se estiver adicionando uma família para um tipo não especificado de hardware, selecione ci_hardware_other. Isso garante que, ao criar novos itens de configuração cujas classes usem a nova família, os atributos apropriados sejam exibidos na guia Atributos. Se você não selecionar o nome de uma tabela no campo Nome da extensão, a tabela padrão é usada e apenas os atributos padrão aparecem ao criar um item de configuração na nova família.
6. Digite uma descrição no campo Descrição.

   A descrição digitada é exibida na Lista de famílias de itens de configuração para fins informativos.
7. Clique em Salvar.

   A família do item de configuração é definida.

Agora que sua nova família está definida, você pode adicionar classes a ela, como descrito em Definir uma nova classe de IC (na página 654).

Construção de uma nova estrutura de atributos

Se nenhuma classe existente ou estrutura da família corresponder a seus requisitos, você poderá recomeçar com um conjunto mínimo de novos atributos. Isso exige a criação de uma nova tabela de extensão e de outras estruturas de suporte.

Antes de usar a interface de administração do CA CMDB para definir uma nova família de IC com base em uma nova tabela de extensão, use o Designer de esquemas do Web Screen Painter para criar a nova tabela de extensão.

Para usar a nova tabela de extensão, você também deve criar novos formulários HTMPL para:

- nova página Detalhes do IC
- nova guia Atributos, com seus atributos associados
- novo formulário de metadados e metadados

O CA CMDB fornece modelos que você pode usar para criar esses formulários HTMPL. As seguintes seções fornecem informações mais detalhadas sobre o que é necessário.

Observação: para procedimentos do Designer de esquemas do Web Screen Painter, consulte o capítulo "Personalização" do *Guia de Implementação do CA Service Desk* e a seção Personalizar o esquema do banco de dados da Ajuda online do Web Screen Painter.

Para usar a nova estrutura na interface de usuário do CA CMDB, defina o seguinte:

- uma ou mais famílias de IC que usam a nova tabela de extensão
- as classes de IC para classificar seus ICs por tipo

Mais informações:

Adição de uma nova família ou classe do CA CMDB (na página 654)

Criar uma nova tabela de extensão

Antes que você possa definir uma família com base em uma nova tabela de extensão, deverá atualizar o banco de dados com a nova tabela, além de atualizar o esquema do CA CMDB com informações sobre essa tabela.

Para criar uma tabela de extensão

1. Usando o Designer de esquemas do Web Screen Painter, defina a nova tabela de extensão e o nome da extensão.
2. Salve e publique a nova tabela de extensão.

Observação: o Designer de esquemas do WSP cria automaticamente o acionador de geração de log no CA CMDB.

Prossiga até a próxima seção para criar a página Detalhes do IC.

Criar uma página Detalhes do IC

Uma página Detalhes do IC é necessária para suportar a exibição de atributo para os ICs associados à nova tabela de extensão.

Para criar a página Detalhes do IC

1. Usando o Designer de esquemas do Web Screen Painter, clique em Arquivo, Novo e crie um formulário com base em detail_extension.template.
2. Salve esse novo formulário como **detail_***extension***.htpml**, onde *extension* é o nome da tabela de extensão.
3. Siga as instruções listadas no arquivo, substituindo a sequência de caracteres ***EXTENSION*** pelo nome da nova tabela de extensão (definido previamente).
4. Salve o arquivo com todas as mudanças.

A página Detalhes do IC inclui duas seções de atributo:

- seção de atributo comum, denominada cmdb_detail.htmpl
- seção específica à família (guia Atributos), denominada nr_cmdb_extension_tab.htmpl, onde *extension* é o nome da nova tabela de extensão.

Prossiga até a próxima seção para criar a guia Atributos do IC (na página 658).

Criar a guia Atributos do IC

A guia Atributos exibe os atributos específicos de família para um IC.

Para criar a guia Atributos

1. Usando o Editor visual do Web Screen Painter, clique em Arquivo, Novo e crie um formulário com base em nr_cmdb_extension_tab.template.
2. Salve o arquivo como **cmdb_cmdb_***extension***_tab.htmpl**, onde *extension* é o nome da nova tabela de extensão.
3. Siga as instruções listadas no arquivo, substituindo a sequência de caracteres ***EXTENSION*** pelo nome da nova tabela de extensão (definido previamente).
4. Salve e publique o arquivo com todas as mudanças.

Prossiga até a próxima seção para preencher a guia Atributos.

Adicionar atributos a formulários

Depois que o Designer de esquemas do Web Screen Painter for usado para criar um novo atributo em uma tabela de extensão, esse atributo deve ser adicionado a qualquer formulário que será usado para exibição ou atualização. Para novos atributos específicos de família, o único formulário que deve ser alterado é a guia Atributos denominada **nr_cmdb_***extension***_tab.htmpl**, onde *extension* é o nome da tabela de extensão. Esse formulário deve ser editado para incluir quaisquer novos atributos.

Para editar um formulário de atributo

1. Usando o Editor visual do Web Screen Painter, clique em Arquivo, Abrir para acessar o formulário apropriado.
2. Arraste e solte os novos atributos no formulário.

   Observação: os formulário fornecidos pelo CA CMDB não podem ser editados pelo Editor visual do Web Screen Painter, assim, use o editor de texto do Web Screen Painter na Origem.

3. Salve e publique o formulário.

Se você ainda não criou um formulário de metadados, prossiga para a seção Criar um formulário de metadados (na página 659). Para definir metadados para um novo atributo no formulário, prossiga até a seção Criar metadados (na página 659).

Criar um formulário de metadados

Uma nova tabela de extensão exige seu próprio formulário de metadados para definir cabeçalhos de coluna e informações de IC padrão para Controle de versão.

Para criar o formulário de metadados

1. Usando o Editor visual do Web Screen Painter, clique em Arquivo, Abrir para acessar cmdb_metadata_extension.template.
2. Salve o arquivo como **cmdb_metadata_***extension***.htpml**, onde *extension* é o nome da nova tabela de extensão.
3. Siga as instruções listadas no arquivo, substituindo a sequência de caracteres ***EXTENSION*** pelo nome da nova tabela de extensão (definido previamente).
4. Salve e publique o formulário com todas as mudanças.

Prossiga até a próxima seção para preencher o formulário de metadados.

Criar metadados

Os metadados incluem informações sobre cabeçalhos de coluna de atributo e IC padrão necessárias para o recurso Controle de versão.

Importante: os metadados exigem planejamento cuidadoso para assegurar os dados corretos em Instantâneos, os títulos corretos em Controle de versão e comparações bem-sucedidas de ICs padrão.

Para criar metadados

1. Usando o Editor visual do Web Screen Painter, clique em Arquivo, Abrir para acessar **cmdb_metadata_***extension***.htpml**, onde *extension* é o nome da tabela de extensão.
2. Seguindo as instruções listadas no formulário, copie e modifique a linha indicada para cada atributo na nova tabela de extensão.

   Observação: os seguintes atributos, embora necessários, não precisam de metadados:

   - ID
   - Last_modified_by
   - Etc (a ser fornecido)

3. Salve e publique todas as mudanças.

Se você adicionar metadados a uma família do CA CMDB existente, as mudanças de auditoria serão exibidas corretamente na guia Controle de versão. No entanto, se você definir metadados para uma nova tabela de extensão, deverá ter uma nova família e classe para seus atributos; para obter mais informações, consulte Adição de uma nova família ou classe do CA CMDB (na página 654).

As estruturas para sua nova tabela de extensão estão agora alocadas. Para definir uma nova família para seus atributos, prossiga para Definir uma nova família do IC (na página 655).

Exemplo:

Neste cenário de exemplo, você criará uma família **Automóvel** e uma classe **Sedan** para rastrear o inventário por fabricação, envio, aluguel, transporte ou outros propósitos. Claro que você também pode criar muitas outras classes de automóvel; este exemplo é apenas para fins de demonstração.

Etapa 1: criar a nova tabela de extensão

1. No Designer de esquemas do Web Screen Painter, clique em Adicionar tabela de extensão.
2. Digite um nome exclusivo para a nova tabela de extensão. Neste exemplo, **vehicle**.

   A tabela de extensão **zvehicle** é criada e suas propriedades exibidas

   Observação: o "z" é anexado ao começo de todos os novos nomes da tabela para distingui-los das tabelas fornecidas pelo aplicativo.
3. Na guia Informações da tabela, defina o campo Grupo de funções para **inventário**. Outros campos são preenchidos com valores padrão.
4. Adicione novas colunas e informações do atributo conforme desejado.
5. Salve e publique a nova tabela de extensão.

Etapa 2: criar uma nova família

Para criar uma família

1. Navegue até Lista de famílias de IC.
2. Clique em Criar novo.

   A página Criar nova família de itens de configuração é exibida.
3. Digite um nome exclusivo para a nova família. Neste exemplo, **Automóvel**.

4. Verifique se Status do registro está definido para Ativo.
5. Selecione o nome da tabela de extensão. Neste exemplo, **zvehicle**.
6. Clique em Salvar.

   A nova família de IC é criada.

Etapa 3: criar uma nova classe

1. Navegue até Lista de classes de IC.
2. Clique em Criar novo.

   A página Criar nova classe de item de configuração é exibida.
3. Digite um nome exclusivo para a nova classe. Neste exemplo, **Sedan**.
4. Verifique se Status do registro está definido para Ativo.
5. Selecione a família. Neste exemplo, **Automóvel**.
6. Clique em Salvar.

   A nova classe de IC é criada.

Etapa 4: criar o novo formulário de detalhes do IC

Para criar o formulário Detalhes do IC

1. No Editor visual do Web Screen Painter, abra o formulário detail_extension.template.
2. Salve o modelo com o nome **detail_zvehicle.htmpl**.

   O novo formulário é salvo em NX_ROOT\site\mods\wsp\project\web\analyst
3. No novo formulário, substitua todas as instâncias de ***EXTENSION*** por **zvehicle**
4. Salve e publique o novo formulário Detalhes do IC.

Etapa 5: criar a guia Atributos

Para criar o formulário da guia Atributos

1. No Editor visual do Web Screen Painter, abra o formulário nr_cmdb_extension_tab.template.
2. Salve o modelo com o nome **nr_cmdb_zvehicle_tab.htmpl**.

   O novo formulário é salvo em NX_ROOT\site\mods\wsp\project\web\analyst
3. No novo formulário, substitua todas as instâncias de ***EXTENSION*** por **zvehicle**
4. Adicione atributos ao formulário como desejado.
5. Salve e publique o formulário da nova guia Atributos.

Etapa 6: criar o formulário de metadados

Para criar o formulário de metadados

1. No Editor visual do Web Screen Painter, abra o formulário cmdb_metadata_extension.template.
2. Salve o modelo com o nome **cmdb_metadata_zvehicle.htmpl**.

   O novo formulário é salvo em NX_ROOT\site\mods\wsp\project\web\analyst
3. Substitua todas as ocorrências de ***EXTENSION*** por **zvehicle**
4. Usando o cabeçalho e espaços reservados para atributo, adicione metadados para todos os atributos específicos de família.
5. Salve e publique o novo formulário de metadados.

CACF (Configuration Audit and Control Facility)

O CACF (Configuration Audit and Control Facility) unifica três disciplinas, Gerenciamento de mudanças, Gerenciamento de configuração (CMDB) e Gerenciamento de detecção para verificar se as mudanças são executadas de forma precisa e se não ocorrem mudanças não autorizadas.

A verificação de mudança ajuda a garantir que o CMDB reflita as mudanças com precisão e as ferramentas de Gerenciamento de detecção verifiquem as mudanças.

A verificação de mudança oferece os seguintes benefícios:

Gerenciamento de mudança

- A garantia de que as mudanças autorizadas sejam corretamente executadas
- Detecção de mudanças executadas de forma incorreta
- A detecção de mudanças não autorizadas.
- Relatórios de gerenciamento
- Auditoria completa de todas as mudanças no nível do atributo
- Detecção de mudanças sobrepostas ou conflitantes

Gerenciamento de configuração

- O CMDB contém uma representação precisa e atual de todos os ICs gerenciados
- Capacidade de exibir o estado futuro do IC com as especificações de mudança propostas
- Auditoria completa de ICs

O CACF contém duas seções principais, a interface administrativa do CMDB e a interface de gerenciamento de mudança que as seções a seguir abordam com mais detalhes.

Mais informações:

Administração e definição de política do CACF (na página 665)
Atributos gerenciados (na página 682)
Estados de mudança gerenciada (na página 682)
Especificações de mudança (na página 685)
Como uma verificação de mudança ocorre (na página 691)
Como arquivar e limpar os dados de auditoria (na página 697)
Implementar uma estratégia de verificação de mudanças (na página 698)
Planejamento e implementação de verificação de mudança (na página 703)
Melhores práticas de verificação de mudanças (na página 711)
Verificar a Atualização do valor do atributo do IC manualmente (na página 715)
Exemplo: Permitir Atualizações informais somente a partir de um Local específico (na página 720)
Exemplo: Atualizar laptops na organização (na página 722)
Exemplo: Bloquear requisições de mudança não verificados (na página 723)
Exemplo: permitir uma Atualização de IC se não houver requisição de mudança correspondente (na página 724)
Exemplo: adiar todas as atualizações do CA Configuration Automation para a TWA (na página 724)
Exemplo: Registrar somente os Resultados da política como um teste (na página 725)
Exemplo: Rejeitar uma atualização de IC (na página 725)
Exemplo: Permitir requisições de mudança criadas sem especificações (na página 726)
Exemplo: Não permitir requisições de mudança criadas sem especificações (na página 727)
Exemplo: permitir inserções informais de fontes selecionadas (na página 727)
Exemplo: permitir uma atualização informal de um IC que não seja de produção (na página 728)

Mais informações:

Como os analistas de mudanças definem as Especificações das mudanças (na página 667)
Verificação de mudança (na página 668)
Como os gerenciadores de mudanças usam as especificações de mudança (na página 669)
Como funciona o CACF (Configuration Audit and Control Facility) (na página 670)

Administração e definição de política do CACF

O Administrador do CMDB define os ICs e atributos que são gerenciados, bem como a política para atualizar os ICs e atributos. Você administra os componentes do CACF no nó de controle da configuração da seção do CA CMDB da guia Administração, define e exibe as especificações de mudança do CACF a partir da Requisição de mudança, do IC, de formulários de incidente ou do nó de Auditoria de configuração na guia Administração.

O administrador deve considerar que permitir mudanças padrão, definir fontes de dados autorizadas e confiáveis, bem como definir quais ICs e atributos de ICs, encontram-se sob a gestão do CACF. Se uma mudança foi executada incorretamente ou se ocorrer uma mudança informal (também conhecida como variação), o CA SDM poderá aceitar o novo valor, criar um incidente ou copiar os dados para a TWA para processamento posterior. O CA SDM pode usar qualquer combinação dessas ações.

Importante: O Administrador de configuração *deve* estabelecer uma estratégia de verificação de mudanças (na página 698) para o ambiente. A política padrão do CACF permite todas as mudanças em todos os ICs, mesmo se ela for informal ou não corresponder a um ticket de mudança.

Você pode implementar políticas de verificação de mudanças de maneira dinâmica ou programadas com antecedência. Você pode definir essas políticas como genéricas ou altamente específicas. A política de verificação da mudança descreve como o CA SDM responde aos seguintes eventos:

Atualizações de MDRs não autorizadas

Indica que MDRs específicos estão autorizados em relação a atributos específicos. O atributo do IC atualiza a partir de MDRs não autorizados, podendo ser aceitas ou rejeitadas de forma seletiva.

Por exemplo, definir políticas para impedir que o CA Application Configuration Manager atualize o endereço IP de um IC, mesmo se houver uma requisição de mudança correspondente. Permitir atualizações ao endereço IP para ocorrer apenas se o MDR de origem for o Spectrum.

Mudanças informais

Detecta e gerencia as atualizações a ICs quando não há uma Requisição de mudança correspondente. Especifique uma política que gerencia mudanças informais solicitando inserções ou atualizações dos dados do IC.

Por exemplo, defina uma política sempre que um IC nomeado de servidor de mudanças* em Nova Iorque, mas que não tem uma requisição de mudança correspondente, não atualize o IC; em vez disso, carregue os dados na TWA.

Mudanças executadas incorretamente

Detecta quando uma requisição de mudança não é implementado (na página 668) corretamente.

As instalações de auditoria proporcionam ao Gerenciador de configurações a capacidade de exibir as mudanças às políticas e as definições de objeto do CACF. O CACF registra cada tentativa de atualização ao IC, sendo tal atualização permitida ou não. Esse log ajuda a determinar qual política permitiu ou proibiu uma mudança em um IC.

O Administrador de configuração define quais status de requisição de mudança representa mudanças editáveis e quais estados de mudança da requisição de mudança representam estados de verificação. Por padrão, é possível editar as especificações de mudança quando a requisição de mudança estiver no estado de mudança da *RDM* e a verificação da mudança ocorrer quando uma requisição de mudança estiver no estado de *Verificação em andamento*. Opcionalmente, os tickets de mudança podem ser automaticamente promovidos ou fechados quando todas as especificações associadas à mudança executarem com êxito.

Importante: Uma possível degradação de desempenho poderá ocorrer se o Administrador de configuração ativar a opção Criar incidente com mais de uma política de verificação ativa.

Observação: por padrão, o CACF considera as atualizações dos valores do atributo para requisições de mudança que tenham verificação de mudança ativa como mudanças não informais, o que é refletido no status Verificação em andamento. O Administrador de configuração pode modificar esse comportamento (na página 682).

Como os analistas de mudanças definem as Especificações das mudanças

A parte da verificação de mudanças da interface de Gerenciamento de mudança integra-se ao formulário de requisição de ticket de mudanças. Normalmente, os analistas de mudanças criam as especificações de mudança ao criar uma requisição de mudança. O analista de mudanças define a mudança em termos de um IC e de um atributo de IC específicos que deseja alterar.

O analista de mudanças pode descrever a especificação de mudança usando qualquer um dos seguintes modelos:

- Fornecer o IC exato, o atributo do IC e o valor.

  Por exemplo, depois que a mudança tiver sido implementada, o endereço IP do server1 define para 10.10.10.10.

- Fornecer o atributo e o valor do IC, mas omitir o nome do IC.

  Por exemplo, depois da mudança, todos os ICs vinculados à requisição de mudança atualizarem para 8 GB de memória.

- Fornecer um valor de atributo para definir quando o atributo não é detectável.

  Por exemplo: após a mudança, o CMDB refletirá que todos os ICs estão localizados em NY.

- Usar o valor detectado.

  Por exemplo, não é possível conhecer o novo endereço IP antes da mudança, mas é possível saber que o endereço IP será definitivamente alterado. Defina o endereço de IP do IC para qualquer valor que o MDR autorizado detectar.

Quando a requisição de mudança é aprovada, as especificações de mudança são aprovadas como parte do mesmo processo de aprovação. Modificações subsequentes à especificação podem ser proibidas e são totalmente auditadas.

Verificação de mudança

A verificação da mudança ajuda a garantir que as requisições de mudança sejam executadas de acordo com especificações de mudança. A verificação ocorre depois que uma requisição de mudança entra em um estado de gerenciamento de mudança como Verificação em andamento e quando qualquer tipo de atualização de IC ocorre. Nesse momento, quando os dados de qualquer MDR ou usuário de cliente web são importados para o CMDB, o CACF compara os dados do atributo de entrada com as especificações ativas de mudança. Se os dados do atributo do IC forem compatíveis, o CACF verifica a mudança. Se os dados de entrada não corresponderem às especificações da requisição de mudança, poderão ser tomadas ações para remediar a variação com base na política.

As políticas executadas podem incluir qualquer uma das ações a seguir:

- Rejeita um única atualização do atributo da transação.
- Rejeita a transação inteira, incluindo todos os pares de atributo e valor.
- Carrega toda a transação na TWA para processamento posterior após a aprovação e a verificação da transação.
- Cria um incidente que descreve cada variação.

  Observação: essa ação poderá acionar notificações e automação existentes. Para evitar a criação de vários incidentes, a detecção de mudanças informais cria um único incidente para todas as mudanças informais em um único IC.
- Aceita a transação incondicionalmente ao aceitar dados de MDRs de origem autorizada.

Por exemplo, o Administrador do CMDB pode definir uma política que cria um incidente quando uma mudança em um servidor de produção for executado incorretamente. Quando os dados importados de um MDR autorizado não corresponderem a uma especificação de mudança pendente, o CACF cria um incidente. A política pode permitir ou rejeitar uma atualização de IC pelos dados de importação incompatíveis. Além disso, o Gerenciador de mudanças pode ter a oportunidade de aceitar o valor recém-detectado, mesmo se o valor não corresponder exatamente à especificação da mudança planejada.

Observação: se ocorrer detecções diversas durante a verificação da especificação da mudança, os dados de detecção podem invalidar uma mudança verificada anteriormente. No final da verificação, o IC está no estado que todas as especificações de mudança desejam.

Como os gerenciadores de mudanças usam as especificações de mudança

O administrador de mudanças pode executar as seguintes ações:

- Exibir e modificar o status de verificação de cada especificação de mudança.

  Por exemplo, o Gerenciador de mudanças deseja saber quais especificações de mudança ainda estão pendentes para a requisição de mudança 12345, que está no status *Verificação pendente*.

- Gerenciar incidentes para mudanças informais ou executadas de forma inadequada.

  Por exemplo, o Gerenciador de mudanças deseja ver quais mudanças falharam na verificação e quais mudanças precisam de mais investigação.

- Gerenciar mudanças que exigem intervenção manual.

  Por exemplo, uma requisição de mudança especifica que é necessária uma verificação manual de uma mudança não detectável e o analista de mudanças deve concluir a tarefa.

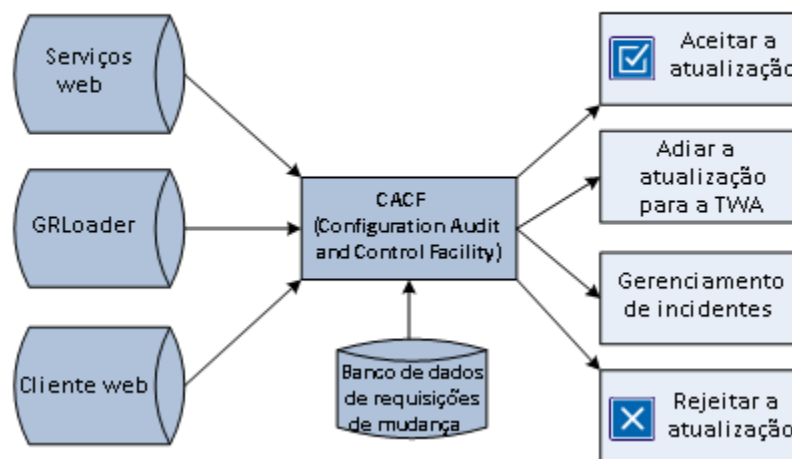
  Por exemplo, o Gerenciador de mudanças investiga e determina que a requisição de mudança 12345 especifica dez especificações de mudança diferentes. Devido a um erro de digitação, a especificação da mudança número 9 estava incorreta e pode ser cancelada.

As instalações de auditoria fornecem os recursos de mudança para exibir o status de cada atualização da especificação de mudança e quaisquer substituições da especificação de mudança. O placar mostra o status do sistema em execução e quaisquer condições que exijam intervenção ou investigação. Os relatório do CA Business Intelligence fornecem uma visão de longo prazo da eficiência das políticas do Gerenciador de configurações para monitorar a integridade do ambiente.

Como funciona o CACF (Configuration Audit and Control Facility)

O CACF controla os dados de entrada do IC antes de carrega-los no CMDB. Essa verificação ajuda a garantir que cada requisição de mudança solicitada seja executada corretamente, detectando e gerenciando as mudanças informais de maneira automática. O Administrador de configuração (Administrador de CMDB) define as políticas de verificação para determinar como o CA SDM responde quando ocorre qualquer desvio ou variação na requisição de mudança solicitada.

O diagrama a seguir mostra como o CACF funciona:

Como funciona o CACF (Configuration Audit and Control Facility)

1. Os dados de entrada do IC são carregados a partir dos Serviços web, do GRLoader, do MDR ou da interface web para solicitar uma atualização do atributo de um IC no CMDB.
2. Com base nas políticas de verificação estabelecidas pelo Administrador de configuração, o CACF conclui uma ou mais das seguintes ações:
   - O CACF aceita a atualização e modifica os dados de CI no CMDB.
   - O CACF adia a atualização à TWA para processamento posterior.

     Por exemplo, o Gerenciador de mudanças lida com as transações na TWA.
   - O CACF cria um incidente e permite que você gerencie o ticket.

     Por exemplo, o processo de Gerenciamento de incidentes precisa gerenciar o incidente para fins de relatório.
   - O CACF rejeita a atualização e os dados de IC não são alterados no banco de dados.

Política de Verificação

Depois que o Gerenciador de configurações e o Gerenciador de mudanças concordam sobre uma política de verificação de mudanças, essas decisões são transcritas para uma política de verificação de mudanças do CA SDM. Um sistema pode ter várias políticas de verificação. Quando uma atualização de IC ocorrer, o CACF seleciona uma única política de verificação para cada atributo atualizado, e essa política pode decidir atualizar o IC. Também pode decidir criar uma entrada na TWA ou criar um incidente sobre a existência de uma especificação de mudança correspondente.

Observação: se você deseja monitorar as atualizações por meio do cliente web, especifique o Padrão da Classe MDR como **Web Client** (diferenciação entre maiúsculas e minúsculas) na política de verificação. Esse uso padrão se aplica às versões em inglês e localizadas do CA SDM quando você deseja monitorar as atualizações por meio do cliente web.

Importante: Determinar quais políticas são necessárias no ambiente requer importante consideração quanto às metas da organização e se deseja introduzir tais políticas.

Seleção da política de verificação

Quando uma atualização ocorrer em um IC, o CACF seleciona uma política para cada atributo atualizado. Essa seleção depende da origem da atualização, do IC de destino e se existe uma especificação de mudança correspondente. Quando várias políticas são compatíveis, o CACF seleciona a única política com a sequência de números mais baixa para gerenciar a atualização do atributo.

Observação: o CACF pode selecionar várias políticas para gerenciar uma única transação que atualiza vários atributos. Por exemplo, a atualização de um IC com uma nova descrição e um novo endereço IP pode acionar duas políticas diferentes.

Cada política tem quatro seções que o CACF utiliza para seleciona-la:

Identificação e prioridade

Identifica uma política e especifica a ordem de avaliação da mesma.

Alinhamento da requisição de mudança

Seleciona as transações com base em quão estritamente a atualização do atributo corresponde a uma especificação de mudança existente.

Filtro de transações

Especifica as fontes de dados às quais a política se aplica.

Filtro do IC

Especifica os ICs aos quais essa política se aplica.

Uma política corresponde a um atualização de atributo quando ele passa cada um desses filtros. Se uma política não corresponde a uma transação, o CACF ignora a política e avalia outras políticas no sistema. Se o CACF ignorar todas as políticas, a ação padrão permite a atualização de atributo do IC ocorra.

Sintaxe do filtro de política de verificação

Para ajudar a estabelecer políticas genéricas, o Alinhamento de requisição de mudança, o Filtro da transação e o Filtro do IC aceitam um asterisco como um caractere padrão final como um curinga. Usar um ponto de exclamação no início desses filtros para indicar a negação.

Importante: As regras de padrão para políticas diferem das regras de valor planejado para a especificação da mudança. Para filtros de políticas, você não poderá usar asteriscos incorporados (*) ou os caracteres especiais de maior que (>) e menor que (<).

Filtros de políticas distinguem maiúsculas e minúsculas para os padrões de seleção da política de verificação, tal como o Nome do IC e a Classe do IC, mesmo se você definir esses atributos com distinção entre maiúsculas de minúsculas.

Observação: um filtro de política em branco "" (sem valor especificado no campo) corresponde somente ao valor em branco, mas um filtro de política que use um asterisco corresponde a todos os valores.

Considere as seguintes informações com os exemplos de políticas de verificação a seguir:

- A Policy1 seleciona o atributo ICs name(prod*) (Endereço IP) onde existe uma especificação de mudança correspondente.
- A Policy2 seleciona o atributo ICs name(prod*) (Endereço IP) onde há uma atualização informal.
- A Policy3 seleciona o nome do Atributo (Memória instalada) dos nomes de ICs (teste*) a partir do mdr (Cohesion).
- A Policy4 seleciona o atributo (Memória instalada) de nome dos ICs ("").

A lista a seguir descreve os possíveis resultados dessas políticas:

- Quando uma atualização ao atributo (Memória instalada) do IC (test2) ocorrer, a Policy3 gerencia a atualização. O CACF ignora a Policy1 e a Policy2.
- Quando uma atualização para o atributo (Memória instalada) do IC (prod3) ocorrer e houver uma especificação de mudança correspondente, a Policy1 gerencia a atualização.
- Quando uma atualização para o atributo (Endereço IP) do IC (development4) ocorrer, o CACF atualiza o IC com o novo endereço IP porque não há uma política correspondente.
- Quando uma atualização para IC (prod1) atributo (Capacidade do disco), não há políticas para o atributo Capacidade do disco) e o CACF atualiza o IC com o novo valor. Nesse exemplo, o CACF *não* gerencia o atributo Capacidade do disco.
- A Policy4 só compara os ICs com nomes em branco. Como os nomes de IC em Branco são inválidos, a mudança nunca será executada.

Priorização de política de verificação pelo Número de sequência

Quando várias políticas correspondem a uma atualização de atributo, o CACF escolhe a política com o número de sequência mais baixo. Considere as seguintes políticas e seus números de sequência.

- IC (prod*) de sequência (1000) do nome da Política (Policy1)
- IC (prod-NY*) de sequência (2000) do nome da Política (Policy2)

Quando uma atualização para IC (prod1), ocorre, a Policy1 gerencia a transação. Quando uma atualização para IC (prod-NY-1) ocorre, Policy1 ainda gerencia a transação porque ela tem um número de sequência mais baixo. Nesse exemplo, a Policy2 nunca entrará em vigor.

É recomendável que você altere os números de sequência para que a política mais específica tenha o número de sequência mais baixo, conforme se vê nos exemplos de políticas a seguir:

- IC (prod*) de sequência (2000) do nome da Política (Policy1)
- IC (prod-NY*) de sequência (1000) do nome da Política (Policy2)

Quando uma atualização para IC (prod1), ocorre, a Policy1 gerencia a transação. Quando uma atualização para IC (prod-NY-1) ocorre, a Policy2 gerencia a transação porque ela tem um número de sequência mais baixo.

Alinhamento da requisição de mudança

Filtro de políticas sobre quão estritamente uma atualização do atributo do IC corresponde a uma especificação de mudança. Depois de uma atualização de IC, o CACF procura por uma especificação de mudança que corresponda tanto ao IC como ao nome do atributo. Essa pesquisa pode verificar a especificação da mudança. Esse Alinhamento da requisição de mudança pode ocorrer como a seguir:

- Há especificações de mudança para esse atributo e IC.
- Há requisições de mudança para esse IC e as requisições de mudança *não* contém especificações de mudança.
- Ocorre uma transação de inserção informal que indica um novo IC. Uma requisição de mudança *não* existe com este IC vinculado a ela.
- Ocorre uma transação de atualização informal que indica um IC existente. Uma requisição de mudança não existe com este IC vinculado a ela.

Somente requisições de mudança em um estado de mudança em que a *verificação da mudança esteja ativa* é que são consideradas ao se procurar por uma requisição de mudança correspondente. Requisições de mudança fechadas, não aprovadas, não programadas ou não executadas não são consideradas ao se procurar por uma requisição de mudança correspondente.

Depois que o CACF determina o alinhamento da requisição de mudança de uma transação, ele faz uma pesquisa por uma política correspondente. Uma política pode gerenciar um ou mais tipos de alinhamento de requisição de mudança:

Requisição de mudança com especificações

Indica que uma requisição de mudança com uma especificação de mudança que indica que existe atualização do IC e o nome do atributo.

Requisição de mudança sem especificações

Indica que as requisições de mudança que especificam esse IC de atualização e tais requisições de mudança não têm nenhuma especificação de mudança.

Inserção informal

Indica um IC inserido; por definição, o IC não possui nenhuma requisição de mudança correspondente em um estado de verificação.

Importante: As políticas que impedem inserções informais devem especificar um atributo gerenciado de *Nome* ou de *Todos os atributos gerenciados*, onde o *Nome* especifica um atributo gerenciado ativo.

O CACF sempre permite inserções e atualizações informais quando uma transação possui apenas atributos não gerenciados.

Atualização informal

Indica um IC atualizado que não possui nenhuma requisição de mudança em um estado de verificação.

Mais informações:

Exemplo: Permitir requisições de mudança criadas sem especificações (na página 726)
Impedir mudanças informais ao atributo. (na página 708)

Exemplo: políticas de alinhamento da requisição de mudança

Os seguintes exemplos de políticas especificam Alinhamentos da requisição de mudança:

- Nome da política (herdado), IC de filtros (*), atributo (Todos os atributos gerenciados), alinhamento (Requisições de mudança sem especificações) e ação (Permitir atualização de Atributo)
- Nome da política (novo), IC de filtros (*), atributo (todos os atributos gerenciados), alinhamento (Requisições de mudança com especificações) e ação (Permitir se corresponder à especificação da mudança)
- Nome da política (autorizada), IC de filtros (*), atributo (todos os atributos gerenciados), alinhamento (inserção ou atualização informal) e ação (cancelar a transação, criar incidente)

Esses exemplos fornecem as seguintes funcionalidades:

- Política (herdada) permite que as requisições de mudança sem especificações do CA SDM r12.6 atualizem o IC, conforme fizeram antes de uma implementação de CACF.
- Política (nova) impõe a verificação da mudança de todas requisições de mudança novas que tenham especificações de mudança correspondentes.
- Política (que não seja informal) impede atualizações em ICs quando não há requisições de mudança em um estado de verificação ativa.

Filtro de transações

Transações com filtro de políticas com base na origem da transação, incluindo o nome de atributo, o nome do MDR, classe de MDR e na função (na página 672)do usuário que executa a atualização.

Observação: se você deseja filtrar usuários conectados por meio da interface web, especifique a palavra-chave **cliente web** para a classe de MDR. A ID do usuário do contato especifica o nome do MDR. Esse método de identificar usuários somente se aplica às políticas de verificação, não sendo exibido em nenhuma outra parte do produto.

Exemplo: filtros de transação

O exemplo de políticas a seguir especifica os filtros de transação:

- Nome da política (root_acesso), ic de filtros (*), atributo (Todos os Atributos gerenciados), função (Administrador), ação (Permitir atualização de Atributo)
- Nome da política (cohesion_not_authorized), IC de filtros (*), atributo (Endereço IP), MDRclass (Cohesion), ação (Manter Valor do atributo anterior)
- Nome da política (John), ic de filtros (user1*), atributo (Todos os Atributos gerenciados), MDRName (user1), MDRClass (cliente web), ação (Permitir atualização de Atributo)

Esses exemplos fornecem as seguintes funcionalidades:

- Política (root_acess), permite que qualquer usuário com acesso de Administrador atualize qualquer valor. Recomendamos que esse tipo de política possua um número de sequência baixo.
- Política (cohesion_not_authorized) evita que qualquer MDR de classe de MDR (Cohesion) atualize o endereço IP do IC filtrado. Esse exemplo mostra como evitar que um MDR não autorizado atualize os dados.
- Política (user1) permite ao user1 atualizar os ICs que o contato possui, mas somente ao usar o cliente web. Esse exemplo mostra como fornecer a usuários específicos o controle total sobre os seus dados.

Filtro do IC

Transações de filtros de política sobre as características do IC atualizado. Esses critérios de seleção incluem Nome de IC, classe, prioridade, tipo de serviço e local.

Importante: O filtro de IC tem base no valor de atributo no IC antes da atualização e não o valor nos dados de entrada da transação.

Exemplo: políticas do filtro de IC

O exemplo de políticas a seguir especifica os filtros de IC:

- Nome da política (priority1), Tipo de serviço dos filtros (priority1 resolution), ação (Permitir atualização somente se houver correspondência com a especificação de mudança, Criar incidente)
- Nome da política (prod-NY), filtros de IC (prod *), local (NY), atributo (Todos os Atributos gerenciada), ação (Permitir atualização somente se houver correspondência com a especificação de mudança)
- Nome da política (prod-not-NY), ic de filtros (prod *), local (!NY), atributo (Todos os atributos gerenciados), ação (Permitir atualização de Atributo)

Esses exemplos fornecem as seguintes funcionalidades:

- Política (priority1), requer ICs com um tipo de serviço de *resolução com priority1* para ter compatibilidade com a requisição de mudança. Essa política é uma prática recomendada porque ajuda a controlar os ICs mais importantes no CMDB para que se torne altamente controlado. Essa política também requer que a verificação de todas as mudanças sob o gerenciamento de mudança tenha especificações de mudanças, devendo estas serem verificadas para estarem concluídas.
- Política (prod-NY) requer que os ICs do local NY tenham requisições de mudança correspondentes. Usar o local para as políticas de filtro pode ajudar a implementar, gradualmente, a verificação da mudança, site por site.
- Política (prod-not-NY) ilustra o uso do ponto de exclamação no padrão de local para indicar os ICs não localizados em NY.

Ações da política

Depois que o CACF seleciona uma política, a seção da ação da política determina o resultado da atualização do atributo. Essa seção identifica a parte mais importante da política de verificação, uma vez que ela afeta a integridade do CMDB. Essa seção também afeta o fluxo de trabalho do gerenciamento de mudança, as notificações relacionadas e os incidentes criados.

Uma política pode ter um dos seguintes comportamentos de atualização:

Permitir atualizar somente se a especificação de mudança for compatível

Condicionalmente aplica-se à atualização de atributos de entrada para o IC se ela corresponde a uma alteração. Essa atualização ocorre quando a requisição de mudança está em um estado de verificação ativa. A seleção dessa opção ativa a verificação da mudança.

Permitir atualização do atributo

Aplica a atualização do atributo de entrada incondicionalmente ao IC. Esta opção desativa de forma eficaz toda a verificação de mudança. Use esse comportamento para mudanças padrão, quando tiver uma origem de dados confiável e autorizada e não precisar de uma requisição de mudança.

Sempre Cancelar toda a transação

Cancela a atualização e qualquer outro atualização de atributo nessa transação, mesmo se houver uma especificação de mudança correspondente. Use esse comportamento para evitar que os MDRs atualizem os ICs em que não têm autorização para atualizar. Se nenhuma política cancelar uma transação, a transação inteira será cancelada, mesmo se outras políticas tiverem permitido que a mudança ocorra.

Por exemplo, especifique esse comportamento para interromper um MDR não autorizado de inserir um IC e também especificar um nome de atributo comum, como *Nome.*

Manter o Valor do atributo anterior

Cancela a atualização do atributo único, mas permite que outros atributos da transação atualizem se a política assim o permitir. Use esse comportamento quando um MDR não tiver autoridade no nível de atributo.

A política de verificação pode especificar que os Incidentes fechem automaticamente quando as verificações falhas são corrigidas. A política pode especificar que os dados da transação de entrada sejam copiados para a TWA. Esse tipo de política é útil quando os dados a partir de um MDR não autorizado requer revisão antes de atualizar o CMDB.

Para permitir que o Gerenciador de configurações identifique que as políticas de CACF criaram o registro da TWA, o campo da requisição de mudança na TWA é definido para o nome da política que o criou. Gravar dados na TWA é ação independente da atualização do IC no CMDB, de modo que uma política pode atualizar o IC, gravar na TWA, ou ambos.

Agendamento de políticas

Você pode especificar as datas de ativação e desativação sobre as políticas de verificação, o que permite ao Administrador de configuração programar mudanças autônomas de política.

Várias políticas

À medida que introduz mais políticas de verificação no ambiente e mais atributos são gerenciados, organizar as políticas torna-se algo cada vez mais complexo, conforme mais sobreposições passam a existir entre as políticas. Por exemplo, há uma política para ICs de Servidor e outra para ICs em NY. Você deve considerar a política apropriada para ICs de Servidor em NY. Use o número de sequência da política para impor a precedência de uma política quando várias políticas tiverem potencial para assumir o controle de um único atributo. Conforme você gerencia mais atributos, a possibilidade de que mais políticas gerenciem uma única transação pode aumentar.

Considere as seguintes informações quando você tiver várias políticas ativas para uma única transação:

- Se nenhuma política selecionada solicita a gravação de dados na TWA, os dados também serão gravados na TWA.
- Se nenhuma política selecionada solicitar o cancelamento da transação, o CACF cancelará a transação inteira.

  Importante: As instalações que usam o serviço web createAsset (incluindo o GRLoader e o CMDBf) desdobram a transação em três transações separadas, duas inserções e uma atualização. Atualizações para ca_owned_resource, pode ser permitido, ao passo que as atualizações para a tabela de extensões do IC são canceladas. Atualizações para os atributos específicos da família do IC na tabela de extensões não podem ser detectadas como inserções, mas como atualizações.

Exemplo: várias políticas

Os exemplos a seguir especificam várias políticas:

- Nome da política (Endereço IP), atributo (Endereço IP), ação (Permitir atualização de Atributo)
- Nome da política (Memória instalada), atributo (Memória instalada), ação (cancelar a transação)
- Nome da política (Capacidade do disco), atributo (Capacidade do Disco), ação (Manter Valor do atributo anterior)

Esses exemplos fornecem as seguintes funcionalidades:

- Se uma transação atualiza apenas o endereço IP, a atualização será realizada.
- Se uma transação somente atualiza a Memória instalada, a atualização não será executada.
- Se uma transação atualiza o endereço IP e a Memória instalada, a transação será cancelada na interface web.
- Se uma transação atualiza o endereço IP e a Capacidade do disco na interface web, o endereço IP será atualizado, mas a capacidade do disco não será atualizada.
- Se uma transação atualiza o endereço IP e a Memória instalada na interface web, nenhum atributo será atualizado.

Consolidação de incidentes

Quando uma política de verificação solicitação para criar um incidente, o CACF pode reduzir o número de incidentes abertos como a seguir:

- O CACF cria apenas um incidente aberto para um único IC para mudanças informais. Mudanças informais adicionais atualizam o único incidente aberto para as mudanças informais.
- O CACF cria apenas uma especificação de incidente aberto para cada falha de verificação na especificação de mudança. Outras falhas de verificação relativas à especificação de mudança atualizam o Incidente aberto.

Atributos gerenciados

Os atributos gerenciados indicam os atributos de IC qualificados para a verificação de mudança pelo CACF. Por padrão, a lista contém o *nome do IC* e *Qualquer atributo gerenciado*. É possível adicionar atributos de IC que deseja que sejam gerenciados como parte de sua estratégia de verificação de mudança. Defina os atributos gerenciados como parte de sua estratégia de verificação de mudanças em Controle da configuração, Nó de atributos gerenciados na seção do CA CMDB da guia Administração.

O CACF não considera os atributos não gerenciados (atributos não listados) para a verificação de mudança. Tais atributos não gerenciados atualizam como de costume.

Importante: A verificação de mudança ignora os atributos não gerenciados e permite que eles atualizem o IC, a menos que uma política de verificação especifique o comportamento Sempre cancelar a transação toda.

Observação: a diferenciação entre maiúsculas e minúsculas na definição do atributo gerenciado aplica-se quando o CACF compara o valor planejado da especificação de mudança com os dados da transação de IC de entrada. A diferenciação entre maiúsculas e minúsculas não se aplica aos padrões de seleção na política, os quais sempre diferenciam maiúsculas de minúsculas.

Para obter uma lista de nomes de atributo de IC, consulte o *Guia de Referência Técnica do CA CMDB*.

Estados de mudança gerenciada

O CACF usa os estados da mudança gerenciada para indicar quais status da requisição de mudança o CACF gerencia. O CACF utiliza estados da mudança gerenciada para controlar como ou quando aplicar a verificação de mudança em relação às atualizações de IC no sistema. É possível personalizar esses estados de mudança para atender às necessidades de sua organização.

É possível configurar os estados de mudança gerenciada na guia Administração no nó do CA CMDB, Controle da configuração, Estados de mudanças gerenciadas.

Observação: o CACF ignora as Requisições de mudança em um estado de Requisição de mudança que está listado nos Estados de mudanças gerenciados.

A lista a seguir descreve as opções de Estados de mudanças gerenciados:

Especificações de mudanças editáveis

Especifica se você pode editar as especificações de mudança de uma requisição de mudança. Em geral, depois que uma requisição de mudança recebe aprovação, você não poderá alterar a solicitação, e as atualizações ficarão restritas a realizar um pequeno conjunto de opções de substituição no estado *Verificação em andamento*.

Verificação de mudança ativa

Especifica se as mudanças detectadas para um IC enquanto a requisição de mudança está com esse status serão consideradas para a verificação da mudança. As requisições de mudança e suas respectivas especificações de mudança são comparadas com quaisquer transações de entrada para verificar se foram executadas com êxito.

O CACF monitora todos os ICs de quaisquer mudanças em seus valores de atributos gerenciados. À medida que o CACF verifica cada mudança do nível do atributo para o IC, o CACF a compara contra uma lista de especificações de mudança que estão em um estado da *verificação de mudança ativa*.

Depois que uma especificação de mudança entra nesse estado, nenhuma especificação de mudança sem um IC específico passa por expansão. Essa expansão ocorre onde novas especificações de mudança são criadas usando a lista de ICs vinculados a requisição de mudança.

Depois que uma especificação de mudança sai desse estado, a lista de especificações de mudança com um status de verificação *Definir após verificar a mudança* é executada. Essa ação atualiza o IC com os valores planejados, conforme especificado em cada especificação de mudança.

Estado de Implementação

Especifica se o estado representa um estado quando as mudanças estão sendo executadas ou implementadas no IC. Quando uma requisição de mudança entrar nesse estado de transição, entende-se que os valores do atributo no IC são voláteis e podem ser atualizados conforme solicitado pelas especificações de mudança pendentes. O CACF não pode considerar essas mudanças como informais; tampouco pode considera-las para verificação final. Normalmente, o processo de verificação de mudança deve comparar somente os dados do atributo de entrada depois que a requisição de mudança for totalmente executada.

Mostrar Botões de substituição de especificação de mudança

Especifica se o analista de mudanças pode controlar as especificações de mudança e que nível de controle é fornecido. Em algumas implementações, o analista de mudanças pode editar especificações de mudança conforme necessário, enquanto em outras implementações o analista de mudanças pode substituir (na página 695) ou cancelar (na página 696) a especificação das mudanças.

Promover requisição de mudança após verificação

Especifica se uma requisição de mudança proporciona para o próximo estado padrão automaticamente após o CACF verificar todas as especificações de mudança.

Estados padrão de mudança gerenciada

Você pode definir os estados da requisição de mudança durante os quais as especificações de mudança são criadas, sobrescritas, verificadas ou ignoradas.

A lista a seguir descreve as definições de estado de mudança gerenciada, fornecidas pelo CA SDM a título de exemplo:

RDM

Definir especificações da requisição de mudança nesse estado; porém, elas não serão consideradas durante a verificação de mudança. As mudanças no IC detectadas enquanto a requisição de mudança está neste estado normalmente são consideradas informais.

Aprovação em andamento

As especificações da mudança nesse estado têm as mesmas características que a RDM, são editáveis e não são consideradas na verificação.

Após a aprovação da requisição de mudança, as especificações de mudança são aprovadas como parte do mesmo processo de aprovação. O CACF proíbe as modificações adicionais à especificação e fornece auditoria completa.

Implementação em andamento

As mudanças aos ICs podem ocorrer, mas não são consideradas como informais nem usadas para verificação. Você pode desejar alterar a definição desse estado de mudança para permitir que ocorra a verificação da Requisição de mudança nesse estado.

Verificação em andamento

As especificações de mudanças não podem ser editadas, mas um analista pode substitui-las. A verificação da mudança está ativa (na página 691) nesse estado.

Mais informações:

Caracteres especiais (na página 687)
Definição de carregamento em massa (na página 689)
Definindo mudanças em massa (na página 689)
Controle de versão do IC e Estado futuro (na página 690)

Especificações de mudança

Uma requisição de mudança contém as especificações da mudança que definem as mudanças específicas do IC que são solicitadas para um IC. O CACF usa essas especificações de mudança quando a requisição de mudança entra em um estado de verificação para validar e confirmar que o número real de mudanças no IC foi concluído corretamente. Cria especificações de mudança a partir de uma requisição de mudança, IC ou Controle da configuração, nó de Especificações de mudança, Seção do CA CMDB da guia Administração.

A especificação de mudança contém as seguintes seções principais:

Número da requisição de mudança

Especifica a requisição de mudança que solicita a mudança.

Nome do CI

Contém o nome do IC que você deseja atualizar.

Você pode deixar o campo Nome do IC em branco para indicar que a especificação da mudança se aplica a todos os ICs definidos para a requisição de mudança. Use essa opção quando todos os itens de configuração de uma requisição de mudança usarem o mesmo atributo gerenciado e valor planejado. A especificação de mudança se aplica a todos os CIs que são vinculados à requisição de mudança quando o status da requisição de mudança for movido para um estado de mudança gerenciada com a verificação da mudança ativa, chamada de expansão.

Nome do atributo

Especifica o nome do atributo gerenciado que você deseja atualizar.

Selecionar Qualquer atributo gerenciado indica que qualquer atributo gerenciado pode mudar durante a verificação da requisição de mudança. Como é possível atualizar vários atributos nesse caso, você não pode especificar o valor planejado.

Valor planejado

Indica o valor esperado do atributo depois de executar a mudança. Depois que a requisição de mudança passa para o estado de verificação e as atualizações de IC pela interface web, pelo GRLoader ou pelos serviços web, o CACF compara o valor planejado com os dados de entrada para determinar uma correspondência.

Caracteres especiais (na página 687) podem ser incorporados no valor planejado quando o valor exato é desconhecido.

Status

Especifica o status da especificação de mudança (na página 693) como Verificação Pendente.

Se não souber o valor planejado antecipadamente, mas sabe que o valor pode mudar, é possível definir o status da especificação de mudança para Usar valores detectados. Esse comportamento requer que a detecção atualize o IC antes do CACF considerar a especificação de mudança como validada. Você precisa desse comportamento para campos numéricos e SRELs onde um asterisco não possa ser aceito como valor planejado.

Para ajuda-lo a definir o valor planejado, a guia Histórico de atributos detectados relaciona todos os valores recém-detectados por um MDR, bem como se foram realmente autorizados, ou carregados no CMDB. Essa guia exibe o formato, a diferenciação de maiúsculas e minúsculas e outras informações sobre valores, de forma que seja possível determinar o padrão do valor planejado adequado.

Caracteres especiais

Você pode incorporar caracteres especiais quando não souber o valor exato. Use o caractere curinga, o asterisco, para correspondência de qualquer número de caracteres. O padrão *deve* corresponder aos dados detectados na mesma sequência e onde os espaços são significativos.

Por exemplo, insira *10.*.*.** como o Valor planejado para corresponder a quaisquer endereços IP que iniciarem com *10.* e que possui dois pontos após qualquer valor entre os pontos.

Por exemplo, o valor de entrada server_type contém o Windows 2003 (WIN32) 5.2.Service Pack 2 (Versão 3790) Intel x86. Para verificar esse valor, especifique um valor planejado ** Service Pack 2 ** na especificação de mudança.

Uma palavra no início do valor planejado indica que valor detectado deve iniciar com aquele valor. Da mesma forma, um asterisco no início do valor planejado indica que o valor detectado pode iniciar com qualquer valor e terminar com o valor especificado após o asterisco.

A tabela a seguir fornece exemplos sobre como usar o asterisco:

Valor planejado	Valor detectado	Correspondente ou Não correspondente
a	b	Não correspondente
a	a	Correspondência
a	aba	Correspondência
a	bab	Correspondência
a*	a	Correspondência
a*	ab	Correspondência
a*	ba	Não correspondente
*a	a	Correspondência
*a	ab	Não correspondente
*a	ba	Correspondência

Um padrão que inicia com um ponto de exclamação resulta na negação do valor. Você só pode usar o ponto de exclamação como o primeiro caractere no padrão. Por exemplo, você não pode usar o padrão de 10.!*.*.*.

Para comparar valores numéricos dentro de valores de sequência de caracteres, use maior que (>) ou menor que (<) como o primeiro caractere no valor planejado. Se houver um ponto de exclamação à esquerda, ele deverá ser o segundo caractere.

Importante: O CACF ignora valores não numéricos à esquerda ou delimitadores nos padrões de valor detectado e de valor planejado.

A tabela a seguir fornece exemplos sobre como usar o ponto de exclamação e os símbolos de maior que e menor que:

Valor planejado	Valor detectado	Correspondente ou Não correspondente
>200	aaa 201 bbb	Correspondência
>200 GB	aaa 200 bbb	Não correspondente
>200 GB	300 GB	Correspondência
!<200 GB	200 Bytes	Correspondência
!<200	200 Bits	Correspondência

Se não souber o valor planejado antecipadamente, mas sabe que o valor pode mudar, é possível definir o status da especificação de mudança para Usar valores detectados. Esse comportamento requer que a detecção atualize o IC antes do CACF considerar a especificação de mudança como validada. Você precisa desse comportamento para campos numéricos e SRELs onde um asterisco não possa ser aceito como valor planejado.

Para ajuda-lo a definir o valor planejado, a guia Histórico de atributos detectados relaciona todos os valores recém-detectados por um MDR, bem como se foram realmente autorizados, ou carregados no CMDB. Essa guia exibe o formato, a diferenciação de maiúsculas e minúsculas e outras informações sobre valores, de forma que seja possível determinar o padrão do valor planejado adequado.

Definição de carregamento em massa

Gerenciar novos ICs sem primeiro criar uma requisição de mudança que requer a definição daqueles ICs, apresenta uma ocorrência dentro de ambientes de CMDB. Considere as seguintes informações ao definir um grande número de ICs.

- Defina uma política especial de carregamento em massa que permita que inserções informais sejam concluídas com êxito, restritas por ID de usuário, MDR ou função.
- Defina uma política especial de carregamento em massa que reencaminhe de todos os novos ICs para a TWA para verificação e processamento posterior. Essa ação também exige a política especial de carregamento em massa anterior.

Definindo mudanças em massa

Criar mudanças idênticas para um grande número de ICs, por exemplo, ao alterar o local de um conjunto de ICs com as seguintes etapas:

1. Criar uma requisição de mudança.
2. Definir uma única especificação de mudança que descreva a mudança e deixar o nome do IC em branco.
3. Anexar todos os ICs à requisição de mudança.

Se você não souber exatamente os detalhes de uma mudança antes da implementação, por exemplo, você adquirir um novo servidor e você só souber o nome do IC, execute as seguintes etapas:

1. Criar uma requisição de mudança.
2. Crie uma especificação de mudança que especifica Qualquer atributo gerenciado como o nome do atributo.
3. Deixe o valor planejado em branco, uma vez que ele é desconhecido.
4. Mova o ticket por meio do processo de gerenciamento de mudança.
5. Quando a requisição de mudança está em um estado de verificação ativo, e a detecção é executada, os dados de entrada do IC são carregados no IC (supondo que a política o permitirá).
6. Quando todas as detecções do IC forem concluídas, o Gerenciador de mudanças deve marcar a especificação de mudança como verificada manualmente.

Siga essas etapas quando há um grande número de diferentes tipos de mudanças a um grande número de ICs. Por exemplo, ao mover um conjunto de servidores de um local para outro e também ao atribuir um endereço IP exclusivo para cada um.

1. Criar requisição de mudança
2. Criar uma planilha e listar em cada linha o número da requisição de mudança, o IC e os novos valores do atributo. Cada linha resulta em uma especificação de mudança diferente.
3. Carregue a planilha com o GRLoader para criar as especificações de mudança necessárias.
4. Promova a requisição de mudança e suas especificações de mudança, como de costume.

Observação: para obter mais informações sobre o GRLoader, consulte o *Guia de Referência Técnica do CA CMDB*.

Controle de versão do IC e Estado futuro

Exibir as especificações de mudança na guia Controle de versão do formulário de Detalhes do IC para fornecer mais informações e identificar a requisição de mudança e as especificações de mudança correspondentes. Essa guia também mostra o estado futuro do IC como se as mudanças fossem aplicadas. Exibir instantâneos do IC, na data programada da requisição de mudança ou, se a requisição de mudança não tiver sido agendada ainda, ele exibe como uma mudança não programada.

O controle de versão ativa as seguintes funções:

- Identificação rápida, sobreposição ou especificação de mudança conflitante.
- Iniciar diretamente na especificação de mudança e exibir os detalhes da mudança correspondente, clicando sobre o link Requisição de mudança, na coluna MDR na exibição de detalhes.
- Instantâneos mostrando *Mudança não programada* indicaram uma mudança que está programada para um momento não especificado no futuro.
- O número da requisição de mudança é exibido com as especificações de mudança mostradas no lado direito do rótulo do instantâneo.

- O texto informativo é exibido na parte inferior do painel, fornecendo as seguintes informações sobre a especificação de mudança como texto sensível ao mouse:
  - Número da requisição de mudança
  - Data da mudança programada, se a requisição de mudança especifica uma data programada
  - Data de necessidade, só aparece se a requisição de mudança especifica uma necessidade por data

Mais informações:

Gerenciando Especificações de mudanças (na página 693)
Status da especificação de mudança (na página 693)
Gerenciando verificações falhas (na página 695)
Gerenciando atributos não detectáveis (na página 696)

Como uma verificação de mudança ocorre

Quando um usuário solicita o salvamento de um IC, o CA SDM pesquisa as especificações de mudança aplicáveis, enquanto pesquisa por todas as correspondências. As informações a seguir descrevem uma especificação de mudança aplicável:

- O IC na especificação de mudança é o mesmo que está sendo salvo.
- A requisição de mudança está em um estado de mudança gerenciada, definido com Verificação de mudança ativa.
- O atributo na especificação de mudança é o mesmo que o atributo que está sendo atualizado.

- A especificação de mudança está ativa
- Se não houver atributos gerenciados sendo atualizados ou política em vigor, o Salvamento prosseguirá sem restrições.

Se os valores dos dados de entrada corresponderem exatamente a uma especificação de mudança, o CACF considera a especificação de mudança como validada. Dependendo da política, a verificação é fecha qualquer Incidente que a verificação de mudanças criou.

A verificação ocorre quando as informações dos clientes web, serviços web ou GRLoader atualizam o IC enquanto a requisição de mudança e todas as especificações de mudança subjacentes estão em processo de verificação. Depois que todas as verificações de uma requisição de mudança forem concluídas, a requisição de mudança poderá, alternativamente, passar para o próximo estado de requisição de mudança automaticamente.

Se os valores dos dados de entrada não corresponderem aos valores na especificação de mudança, ele será considerado como incorretamente implementado ou tendo falhado em alterar e os Incidentes são criando ou vinculados a, dependendo da política.

Por exemplo, o CA SDM não encontra as especificações de mudança aplicáveis, mas há requisições de mudança em um estado de *verificação de mudança ativo*. Essas requisições de mudança especificam o IC de destino e não tem especificações de mudança. O CACF gerencia essa mudança por meio de políticas que lidam com *Requisições de mudança sem especificações*.

- Se não houver nenhuma especificação de mudança aplicável nem requisição de mudança sem especificações, a operação de salvamento é considerada como informal.
- Depois que todos os atributos tiverem sido processados, nenhuma política que solicitou que os dados de entrada fossem gravados nos disparadores da TWA.

Gerenciando Especificações de mudanças

Depois que uma mudança foi executada ou implementada, a requisição de mudança entra em um estado de mudança que é gerenciado pelo CACF e cujo estado de mudança está definido com *Verificação de mudança ativa*. Quando a requisição de mudança está nesse estado, o CACF analisa todas as atividades de IC relacionadas e informa o status de cada especificação de mudança no placar.

O placar é usado pelo Gerenciador de mudanças para verificar se as mudanças necessárias foram executadas corretamente, bem como para executar verificações manuais que foram solicitadas por requisições de mudança.

Depois que todas as verificações de uma requisição de mudança estiverem concluídas, a requisição de mudança poderá, opcionalmente, passar automaticamente para o próximo estado da requisição (normalmente fechado), onde todas as especificações de mudança serão automaticamente marcadas como inativas.

Status da especificação de mudança

As especificações de mudança usam o status para indicar o tipo de verificação a ser executado e o estado atual da verificação. Os valores de status são usados também no log de verificação ao registrar as operações de verificação de mudanças durante o processo de verificação.

Status inicial

Usado ao criar uma especificação de mudança para especificar o tipo de verificação para o CACF executar. Esses status não são finais e a requisição de mudança não é considerada verificada quando as especificações de mudança não estão em nenhum desses status.

Verificação pendente: a especificação de mudança não foi verificada ou a mudança está aguardando que o IC atualize.

Verificação manual será necessária: quando as mudanças de uma requisição de mudança forem verificadas, uma verificação manual será necessária.

Usar valores detectados: copiar o valor detectado para o IC no momento da verificação e usado quando o valor planejado não for conhecido antes da verificação.

Definir depois de executar mudança: define um atributo do IC para o valor planejado depois que a verificação foi concluída. Use este status para definir os atributos de IC quando o atributo não for detectável. Por exemplo, definir o Contato primário do IC para User1 depois que uma mudança é concluída.

Status final

Indica que uma especificação de mudança foi concluída e é considerada como final. Quando todas as especificações de mudança entrarem em um desses estados finais, as Requisições de mudança serão elegíveis para promoção para o próximo estado padrão.

Verificado: a especificação de mudança foi verificada com êxito.

Foi manualmente verificada: a especificação de mudança foi manualmente verificada.

Valor detectado utilizado: o IC foi atualizado com o valor detectado.

Foi definido para o valor planejado: o IC foi atualizado com o valor planejado após a verificação da requisição de mudança.

Valor planejado aceito: o IC foi atualizado com o valor planejado e substituído durante a verificação.

Valor detectado aceito: o IC foi atualizado com o valor atualizado com o último valor detectado e sobrescrito durante a verificação.

Nenhuma mudança: o valor planejado correspondeu ao IC no momento da verificação e nenhuma verificação foi necessária.

Cancelar: a especificação de mudança foi cancelada (na página 695) pelo gerenciador de mudanças.

Status de intervenção

Indica que uma especificação de mudança requer intervenção manual para verificação. O CA SDM destaca os status em vermelho nos formulários de lista. Esses status não são finais e a requisição de mudança não é considerada verificada quando as especificações de mudança estão em qualquer um desses status.

Falha na verificação: a detecção encontrou um valor diferente do que foi especificado na requisição de mudança. O analista de mudanças deve determinar se a mudança foi corretamente executada e a requisição de mudança foi especificada de forma incorreta, ou se a requisição de mudança estava correta e se a mudança exige nova verificação. Dependendo da definição do Estado da mudança gerenciada e do status atual da requisição de mudança, o Analista de mudanças pode substituir, alterar ou cancelar a especificação de mudança que falhou.

Verificação manual ativa: a verificação manual é necessária antes que a especificação de mudança possa ser marcada como final.

O Status substitui a ação

Indica uma ação para iniciar durante a verificação de mudança. Esses status não são finais e a requisição de mudança não é considerada verificada quando as especificações de mudança estão em qualquer um desses status.

Aceitar valor planejado - solicitação para substituir o atributo do IC com o valor planejado.

Aceitar valor detectado - solicitação para substituir o atributo do IC com o último valor detectado.

Status de relatórios

Indica o resultado das operações da política que o log de verificação exibe para fins de registro e não são usadas pelas especificações da mudança.

Atualização foi permitida: uma política permitiu uma solicitação para atualizar um IC e não correspondeu a nenhuma especificação de mudança.

Gerenciando verificações falhas

Quando uma verificação falha, o CMDB, a Auditoria de configuração, o nó de Verificações falhas no placar relaciona o número de verificações que falharam e as especificações de mudança que exigem intervenção manual em vermelho. As especificações de mudança também podem ser exibidas na guia Especificações de mudança na requisição de mudança, IC ou guia Administração com o status de verificação Verificação falhou. Quando uma verificação falha, o analista de mudanças pode interferir ou aguardar até a próxima detecção.

Se o estado da mudança gerenciada permite a ação do botão Mostrar substituição da especificação da mudança, o analista de mudanças pode abrir a especificação de mudança, revisar os dados e, em seguida, clicar em uma das opções a seguir para fechar a verificação, movendo-a para um estado final:

Aceitar valor descoberto

O analista determina que a especificação da mudança está incorreta e que a ferramenta de detecção detectou o valor correto.

Aceitar valor planejado

O analista determina que a ferramenta de detecção está incorreta ou não realizou a detecção, bem como para aceitar o valor planejado, como se ele tivesse sido detectado corretamente.

Cancelar

Essa parte da requisição de mudança não foi executada e a especificação foi cancelada.

Gerenciando atributos não detectáveis

Quando uma Especificação de mudança exige a verificação manual, o Analista de configuração deve verificar a mudança manualmente. O CMDB, a Auditoria de configuração, o nó de Intervenção manual no placar mostram o número de especificações de mudanças que exigem intervenção manual em vermelho. As especificações de mudança também podem ser exibidas na guia Especificações de mudança na requisição de mudança, IC ou guia Administração com o status de verificação Verificação manual falhou.

Se o estado da mudança gerenciada permite a ação do botão Mostrar substituição da especificação da mudança, o analista de mudanças pode abrir a especificação de mudança, revisar os dados e, em seguida, clicar em uma das opções a seguir para fechar a verificação, movendo-a para um estado final:

Marcar como verificado

Usado quando o atributo não é detectável e manualmente verificado.

Cancelar

Essa parte da requisição de mudança não foi executada e a especificação foi cancelada.

Como arquivar e limpar os dados de auditoria

Recomendamos que você faça o arquivamento e eliminação das entradas de log de verificação, o histórico de auditoria do CACF e o histórico de auditoria do IC como parte de sua manutenção periódica do banco de dados.

Importante: Os relatório do CACF do CA Business Intelligence normalmente apresentam relatórios mensais com um resumo anual. O valor padrão do tempo de eliminação de arquivo das regras de eliminação de arquivos de log, o histórico de auditoria do CACF e as tabelas do histórico de auditoria de IC é de 30 dias. Use o mesmo valor no regras de arquivamento e eliminação para garantir a consistência dos dados entre as entradas do log de verificação, Incidentes e Requisições de mudança. É possível alterar o padrão de 30 dias para algo mais para dar conta de seus requisitos de geração de relatórios.

Execute as ações a seguir para arquivar e eliminar dados de auditoria:

1. Use a regra de incidente atual para arquivamento e eliminação de incidentes inativos ou mais antigos que *nn* dias.

   O CA SDM arquiva e elimina entradas de log de verificação somente após arquivamento e eliminação dos incidentes associados. Se associar uma requisição de mudança com um incidente, o CA SDM não verificará se a requisição de mudança está ativa.

2. Usar a regra atual da requisição de mudança para arquivamento e eliminação de requisições de mudança inativas ou mais antigas que *nn* dias.

   O CA SDM arquiva e elimina as entradas do log de verificação e as especificações de mudança somente após arquivamento e eliminação das requisições de mudança associadas. Se você associou um incidente a uma requisição de mudança, o CA SDM não arquivará, nem eliminará a requisição de mudança.

3. Usar a regra Log de verificações de mudanças informais para as mudanças informais que não geraram um incidente.

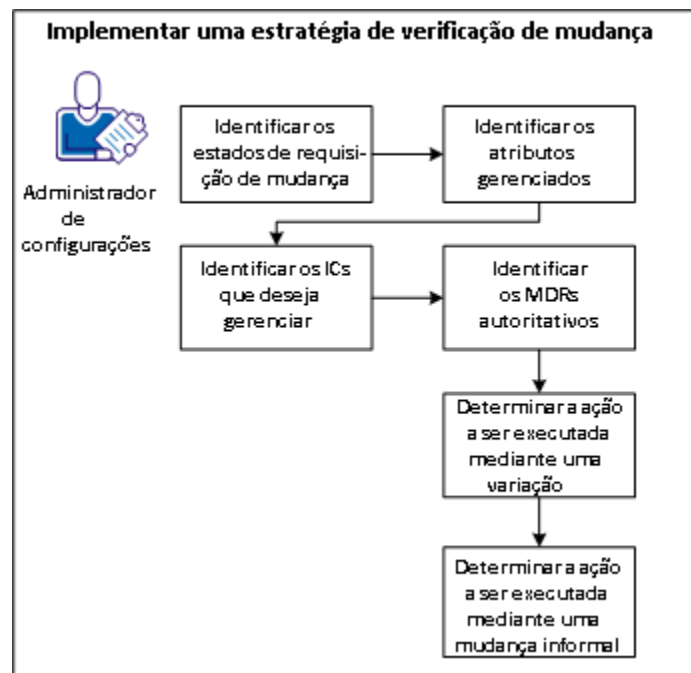
   Use esta regra para arquivamento e eliminação de entradas de log de verificação mais antigos que *nn* dias. Por definição, as mudanças informais não são associadas às requisições de mudança.

4. Usar a regra CMDB Audit para arquivamento das informações mostradas nas guias Histórico de especificação de mudança, Histórico de política de verificação, Histórico de estado de mudança gerenciada e Histórico de atributo gerenciado nos respectivos formulários detalhados de Especificações de mudanças, Política de verificação Estado de mudança gerenciada e Atributos gerenciados. O CA SDM armazena essas informações na tabela ci_audit.

Implementar uma estratégia de verificação de mudanças

O Administrador de configuração determina com que agressividade se deve implementar a estratégia de verificação de mudanças no ambiente CMDB. Você deve identificar as áreas de seu processo de Gerenciamento de mudança que necessitam de uma estratégia de verificação de mudanças. Essas áreas incluem atributos sob o controle de mudanças, os estados de requisição de mudança que indicam que a verificação de mudanças está ativa, quando poderá modificar a especificação da mudança e MDRs autorizados.

Por exemplo, você só deseja permitir atualizações ao atributo de endereço IP a partir do MDR1. Também é possível determinar as ações apropriadas quando o CACF detecta uma variação e uma mudança informal.

O diagrama a seguir explica como a Administração de configurações implementa uma estratégia de verificação de mudanças:

1. Identificar os estados de requisição de mudança (na página 699).
2. Identificar os atributos gerenciados (na página 699).
3. Identificar os ICs que você deseja gerenciar (na página 700).
4. Identificar os MDRs autorizados (na página 701).
5. Determinar a ação de uma variação (na página 702).
6. Determinar a ação de uma mudança informal (na página 702).

Identificar os estados de requisição de mudança.

O Administrador de configuração identifica a requisição de mudança em relação a quando a verificação da mudança estará em vigor para o IC depois que a mudança for executada. Os estados de mudança ajudam a determinar condições específicas, como se você pudesse editar as especificações de mudança em um estado particular. Por exemplo, se você quiser revisar o estado de mudança da RDM das requisições de mudança que solicitam atualizações para os ICs.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da Configuração, Estados de mudança gerenciada.
2. Clique em RDM para exibir os detalhes de estado mudança ou criar um estado de requisição de mudança que ainda não tenha sido definido.

   Observação: por padrão, o estado da requisição de mudança – RDM permite editar somente as especificações de mudança. O estado da Implementação em andamento não permite editar as especificações de mudança. O estado da Verificação em andamento, ativa a verificação da mudança e exibe os botões de substituição do Gerenciador de mudanças ou outro usuário autorizado.

3. Especifique as opções de CACF e o comportamento para quando uma requisição de mudança entrar neste estado.
4. Clique em Salvar.

Identificar os atributos gerenciados.

Identifique quais atributos de CI você deseja gerenciar em relação à estratégia de verificação de mudanças. Por exemplo, você deseja gerenciar o atributo endereço IP (alarm_id) com a verificação de mudança.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da Configuração, Atributos gerenciados.
2. Clique em Criar novo.
3. Conclua as seguintes etapas:
   a. Digite **alarm_id** como o Nome do atributo
   b. Digite o **endereço IP** como o Rótulo do atributo.

c. Selecione um status de verificação inicial na lista suspensa.

   Padrão: verificação pendente

d. (Opcional) Selecione a opção que diferencia maiúsculas e minúsculas, se você deseja aplicar a diferenciação de maiúsculas e minúsculas em comparações de valor planejado de especificações de mudança.

   Padrão: desativado

e. Clique em Salvar.

Identificar os ICs que você deseja gerenciar.

Identificar os ICs que deseja gerenciar com uma política de verificação. Por exemplo, você deseja gerenciar o endereço IP (alarm_id) de todos os ICs de alta prioridade com nomes que começam com NY_Server.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da configuração, Políticas de verificação.
2. Clique em Criar novo.
3. Conclua as seguintes etapas:
   a. Insira uma sequência, como **100.**
   b. Digite **Endereços IP do servidor NY**, como nome da política.
   c. Selecione as devidas opções de alinhamento de requisição de mudança.

      Por exemplo, você deseja que a política de verificação para todas as opções exceto as Especificações sem requisições de mudança.
4. Execute as etapas a seguir para especificar a transação e filtros de IC:
   a. Selecionar o endereço IP na lista suspensa Atributo gerenciado.
   b. Digite um Padrão de função ou deixe o asterisco para aplicar a todas as funções.

c. Digite **NY** como o Padrão de local.

d. Digite **NY_Server*** como o nome do Padrão de IC.

   Por exemplo, esse filtro verifica ICs nomeados NY_Server1, NY_Server2, e assim por diante.

5. Selecione *Permitir atualizar somente se corresponder à especificação* da mudança a partir da lista suspensa Atualizar comportamento.
6. (Opcional) Use o modo de Somente log se você quiser experimentar com a política e exibir os resultados somente no log padrão e não afetar o ambiente CMDB ativo.
7. Clique em Salvar.

Identificar os MDRs autorizados.

Identificar os MDRs autorizados no ambiente CMDB. Por exemplo, você deseja permitir atualizações a ICs do CA Configuration Automation que você identificou como o MDR1. Você considera as atualizações dos serviços web que você identificou como MDR2 como não autorizadas e deseja enviar tais solicitação para a TWA.

Siga estas etapas:

1. Abra a política Endereços IP do servidor NY e, em seguida, clique em Editar.
2. Digite o **MDR1** como o Padrão de nome do MDR.

   Observação: se você deseja excluir um MDR chamado MDR2, mas você deseja permitir que o MDR1, MDR3, e assim por diante, digite **!MDR2** como padrão.

3. Criar uma nova política de verificação, como Servidor NY MDR2.
4. Insira as mesmas informações que as da política anterior, exceto os seguintes campos:
   a. Digite o **MDR2** como o Padrão de nome do MDR.
   b. Selecione *Cancelar sempre a transação toda* como Comportamento de atualização.
   c. Selecione Sempre a partir da lista suspensa Gravar dados na TWA.
5. Clique em Salvar.

Determinar a Ação de uma variação.

Determinar a ação de uma variação. Por exemplo, uma mudança em um IC não coincide com os valores especificados na requisição de mudança. Você deseja que a política de verificação crie um Incidente para a variação.

Siga estas etapas:

1. Abra a política Servidor NY MDR2 que você criou e clique em Editar.
2. Selecione Sim na lista suspensa Criar incidente e atribua um modelo.
3. Clique em Salvar.
4. Um usuário final cria uma requisição de mudança com uma especificação de mudança para atualizar um IC no MDR2.
5. O CACF cria um incidente se o MDR2 solicitar uma atualização de IC com um valor que não corresponde ao valor planejado na especificação de mudança, definido na requisição de mudança.

Determinar a ação de uma mudança informal.

Determinar a ação de uma mudança informal. Por exemplo, o CACF detecta uma mudança em um IC que não tem nenhuma especificação de mudança a partir de uma requisição de mudança ativa. O Administrador de configuração deseja rejeitar esses tipos de solicitações.

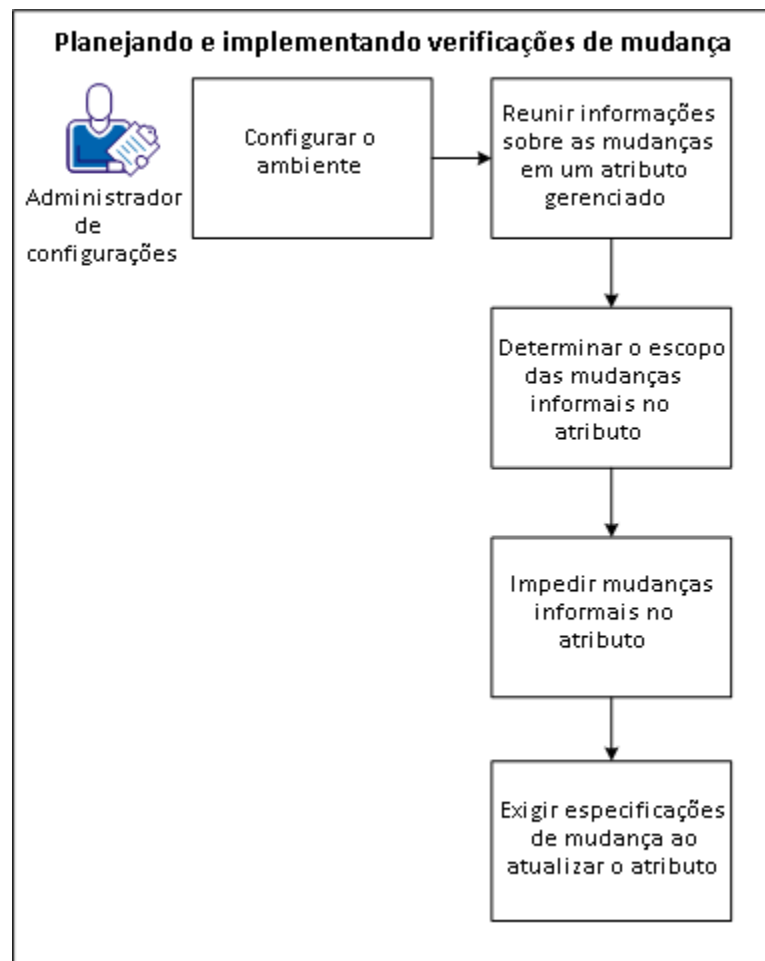
Siga estas etapas:

1. Crie uma política de verificação e digite **Servidor NY informal** como nome.
2. Preencha os campos do padrão apropriado.
3. Certifique-se de que apenas Inserção informal e Atualização informal estejam selecionadas como opções de Alinhamento da requisição de mudança.
4. Selecione *Permitir atualizar somente se corresponder à especificação* da mudança a partir da lista suspensa Atualizar comportamento.
5. Selecione Sim na lista suspensa Criar incidente e atribua um modelo.
6. Clique em Salvar.

Planejamento e implementação de verificação de mudança

O Gerenciador de configurações deseja implementar a verificação de mudança, para que o CMDB contenha os dados corretos. O Gerenciador de mudanças deseja ajudar a garantir que as mudanças sejam executadas corretamente e preocupa-se com mudanças informais, bem como em compreender o número de mudanças informais que ocorrem e de quais fontes de dados. Os gerenciadores de mudanças concordam que implementar a verificação de mudanças proporciona um valor significativo para a organização. O Gerenciador de mudanças deseja ajudar a garantir que nenhuma mudança no processo de Gerenciamento de mudança prejudique o ambiente de produção.

O Gerenciador de configurações e o Gerenciador de mudanças concordam quanto a uma implementação faseada e conservadora, de modo que um administrador de configuração implementa políticas para determinados locais e ICs específicos nesses locais. Esse cenário descreve exemplos de fases sobre a conclusão da implementação da política de verificação para um público mais amplo de sua organização.

O diagrama a seguir mostra como um Administrador de configuração conclui o exemplo de fases para implementar a verificação de mudanças:

1. Configurar o ambiente (na página 705).
2. Coletar informações sobre mudanças em um atributo gerenciado (na página 706).
3. Determinar o escopo das mudanças informais no atributo (na página 707).
4. Impedir mudanças informais ao atributo (na página 708).
5. Exigir Especificações da mudança ao atualizar o atributo (na página 710).

Configurar o ambiente.

Você pode configurar o ambiente para que os Administradores de configuração sempre possam atualizar ICs. O Administrador de configuração pode criar e atualizar itens de configuração no CMDB, conforme necessário, sem que seja necessário especificar uma requisição de mudança e é confiável para o fornecimento dos dados de configuração corretos.

Siga estas etapas:

1. Criar uma política de verificação chamada **Policy0.1** com as seguintes informações:
   - Digite **1** como a sequência.
   - Digite o **Permitir que o administrador sempre atualize ICs** como a descrição.
   - Selecione todas as opções de Alinhamento da requisição de mudança.
   - Digite a **Administrador de configurações** como Padrão de função.
   - Insira **Cliente web** como Padrão de classe do MDR.
   - Digite um asterisco (*****) como o Nome do IC e a Classe, e todos os outros padrões.
   - Selecione Qualquer atributo gerenciado para o Atributo gerenciado.
2. Selecione Permitir atualização como ação do Comportamento de atualização.
3. Clique em Salvar.

   A política é ativada para permitir que somente Administradores de configuração atualizem os ICs, sempre.

Colete informações sobre mudanças em um atributo gerenciado.

Você deseja obter informações sobre as mudanças de um atributo gerenciado de IC para identificar, quais ICs estão sendo atualizados, quais são as fontes das mudanças, quem está fazendo as mudanças e os valores que estão sendo especificados para ajudar ao definir uma estratégia de verificação para o atributo e ICs correspondentes. Por exemplo, se você quiser entender o escopo de todas as mudanças para o endereço IP (alarm_id) e registrar isso no log padrão do CA SDM (stdlog). A coleta dessas informações pode levar várias semanas, dependendo do número de mudanças feitas aos atributos que ocorrem em sua organização.

1. Definir Endereço IP (alarm_id), como um atributo gerenciado.
2. Definir implementação em andamento e Verificação em andamento como Estados de mudança gerenciada no seu ambiente e ativar a Verificação ativa em ambos os estados.
3. Criar uma política de verificação chamada Policy1.1 com as seguintes informações:
   - Digite **3000** como a Sequência.
   - Digite **Registrar todas as mudanças para o endereço IP** como a descrição.
   - Selecione todas as opções de Alinhamento da requisição de mudança.
   - Digite um asterisco como o Nome do IC e a Classe e todos os outros padrões.
   - Ativar o Modo de apenas log.
4. Clique em Salvar.
5. Após algumas semanas, revise os stdlogs para exibir as origens das atualizações.

   Por exemplo, o log exibe as atualizações de IC informais e as atualizações com requisições de mudança correspondentes.
6. É possível determinar que usuários localizados em NY atualizem o endereço IP dos CIs sem criar requisições de mudança.
7. Após concluir a análise, desative Policy1.1 editando a política e definindo como? como Inativo.

Determinar o escopo das mudanças informais no atributo.

Você deseja determinar o escopo das mudanças informais no atributo Endereço IP. Conhecer o escopo das mudanças informais ajuda a compreender seu impacto na organização. Por exemplo, com base na sua análise anterior usando a opção Somente log, você pode criar incidentes sempre que ocorrer uma mudança no endereço IP para ICs que começam com test localizado em NY sem uma requisição de mudança. Comunicar com os gerenciadores de mudanças em sua organização para ignorar os novos Incidentes que esse processo criar.

Siga estas etapas:

1. Execute a seguinte ações da implementação inicial:
   - Definir Implementação em andamento como um estado de mudança gerenciada e ativar a opção Estado de Implementação.
   - Definir Verificação em andamento, como um estado de mudanças gerenciadas e desativar a opção Promover requisição de mudança após verificação. .
   - Definir Endereço IP (alarm_id), como um atributo gerenciado se já não estiver definido.
2. Criar uma política de verificação chamada Policy2.1 com as seguintes informações:
   - Digite 3001 como a Sequência.
   - Digite uma descrição sobre essa política. Por exemplo, se você digitar **Inserções informais, as atualizações informais farão com que sejam criados Incidentes. Todas as outras mudanças não serão impedidas**.
   - Selecionar Atualizações informais e Inserções informais como alinhamentos.
   - Selecionar o endereço IP na lista suspensa Atributo gerenciado.
   - Digite **test*** como o Nome do IC, **NY** como Local e um asterisco para todos os demais Padrões.
   - Selecione Permitir atualização do atributo, Sim para Criar incidente, e um Modelo de incidente a partir das ações.
3. Clique em Salvar.

Depois de concluir essa fase, o CACF cria incidentes para todos os computadores em NY. É possível descobrir as informações a seguir, depois de verificar os incidentes:

- Vários endereços IP diferentes de relatórios de MDRs para o mesmo IC.
- Alguns MDRs são autorizados, outros não.
- Alguns ICs não devem ser gerenciados com base em local, família, Nome, Tipo de serviço e assim por diante.

4. O Gerenciador de mudanças se reúne com outros Gerentes de para revisar o CMDB, os formulários de detalhes do IC, os Logs de verificação e a filtragem por nome de atributo para ver os dados informais.
5. A sua organização decide atualizar o filtro de IC na Política 2.1 para gerenciar Servidores de prioridade 1.

Impedir mudanças informais ao atributo.

Você deseja impedir que mudanças informais no atributo Endereço IP para ajudar a garantir a integridade dos dados do CMDB e necessita de uma requisição de mudança para a atualização. A requisição de mudança deve especificar o IC e uma especificação de mudança não é necessária para o endereço IP para que a mudança ocorra. A verificação de mudança ocorre no nível da requisição de mudança/IC, mas não no nível de atributo. Por exemplo, evitar quaisquer atualizações informais e usar a criação de incidentes para rastrear os usuários que solicitam essas mudanças.

Siga estas etapas:

1. Definir Policy1.1 e Policy2.1 para Inativo e desativar essas políticas, de modo que elas não estejam em vigor.
2. Criar a Policy 3.1 com as seguintes informações:
   - Digite **3100** como a Sequência.
   - Digite **Impedir mudanças informais sem nenhuma requisição de mudança** como descrição.
   - Selecione Atualização informal como alinhamento.
   - Digite **test*** como o Nome do IC e **NY** como Local, Qualquer atributo gerenciado e um asterisco para todos os Padrões.
   - Selecione Sempre Cancelar toda a transação.
3. Clique em Salvar.

4. Criar a Policy3.2 com as seguintes informações:
   - Digite **3200** como a Sequência.
   - Digite **Exigir uma requisição de mudança para as mudanças de endereço IP** como a descrição.
   - Selecione Requisições de mudança sem especificações como o alinhamento.
   - Digite **test*** como o Nome do IC, **NY** como Local e um asterisco para todos os demais Padrões.
   - Selecionar o endereço IP na lista suspensa Atributo gerenciado.
   - Selecione Permitir atualização do Atributo como ação.
5. Clique em Salvar.

   Essa política elimina as mudanças informais, uma vez que as requisições de mudança devem acompanhar a mudança.

   O Gerenciador de configurações percebe que os dados não definidos na requisição de mudança também estão sendo atualizados, uma vez que as especificações de mudança não são necessárias para as mudanças no nível de atributo. Por exemplo, solicitar uma mudança para aumentar a Memória instalada ao mesmo tempo em que se altera o endereço IP não seria considerado uma mudança informal porque há uma requisição de mudança. Eles também gostariam que as requisições de mudança fossem automaticamente verificadas e promovidas e determinam que querem a verificação no nível de atributo.

Exigir especificações da mudança ao atualizar o atributo.

O Gerenciador de configurações demonstra preocupação quanto aos dados nos CMDB receberem diversas atualizações de mudanças não especificadas na requisição de mudança. Por exemplo, um usuário altera o valor da Memória instalada (phys_mem) e o endereço IP (endereço_ip) ao mesmo tempo. Na fase anterior, o CACF não considera essa solicitação como uma mudança informal, pois existe uma requisição de mudança.

O Gerenciador de configurações aplica a verificação de mudança no nível do atributo. O administrador de configurações cria uma política que exige o uso de especificações de mudança ao atualizar o endereço IP e para criar um incidente se não houver tentativas de atualizações informais.

Siga estas etapas:

1. O Gerenciador de configurações entra em contato com os analistas de mudanças para dizer que as mudanças no Endereço IP devem conter uma especificação de mudança.
2. Definir Policy3.1 e Policy3.2 para Inativo para desativar essas políticas, de modo que não estejam em vigor.
3. Criar a Policy4.1 com as seguintes informações:
   - Digite **4000** como a Sequência.
   - Digite **Exigir especificações de mudança para as mudanças de endereço IP** como a descrição.
   - Selecione Inserção informal, Atualização informal e Requisições de mudança sem especificações como alinhamento.
   - Digite **test*** como o Nome do IC, **NY** como Local e um asterisco para todos os demais Padrões.
   - Selecionar o endereço IP na lista suspensa Atributo gerenciado.
   - Selecione Sempre cancelar toda a transação como a ação.
4. Clique em Salvar.
5. Criar a Policy4.2 com as seguintes informações:
   - Digite **4100** como a Sequência.
   - Digite **Exigir especificações de mudança para as mudanças de endereço IP** como a descrição.
   - Selecione Requisições de mudança com especificações como o alinhamento.

- Digite **test*** como o Nome do IC e **NY** como padrão de local.
- Selecionar o endereço IP na lista suspensa Atributo gerenciado.
- Selecione Permitir Atualizar apenas se a mudança corresponde à Especificação da mudança como ação.

6. Clique em Salvar.

Você concluiu com êxito as etapas de exemplo para implementar a verificação de mudanças em seu ambiente. Você pode expandir a estratégia de verificação de mudanças para incluir mais atributos, ICs, MDRs e inquilinos.

Melhores práticas de verificação de mudanças

Considere as práticas recomendadas a seguir ao implementar a verificação de mudanças:

- Definir um número pequeno de políticas.
- Evite o uso de lógica negativa (ponto de exclamação em um padrão de política).
- Um único salvamento da atualização de IC deve corresponder a um pequeno número de políticas.
- Organizar as políticas em uma estrutura por níveis numerados.
- Use as políticas de Modo Somente log antes de implementar uma política de verificação de mudanças.
- Minimizar as políticas de sobreposição, nas quais várias políticas gerenciam um único atributo que está sendo atualizado.
- Limitar o número de incidentes que o CACF cria.
- Implemente arquivamento e eliminação de dados do CACF.

Mais informações:

Organização de políticas (na página 712)
Considerações sobre o Multi-Tenancy (na página 713)
Funções do CACF e acesso funcional (na página 713)

Organização de políticas

É possível usar várias estratégias para manter o controle das políticas. Recomendamos o uso de uma abordagem em vários níveis. Usar incrementos de 100 entre números de política para permitir futuras inserções.

Considere o seguinte exemplo de níveis para essa estratégia:

Políticas fundamentais

100.000 - 199.999

- Permitir que os Administradores de mudança façam inserções
- Proibir inserções pela Classe de MDR (xxxx)
- Excluir todos os ICs de teste da criação de incidentes

Políticas temporárias ou provisórias

200.000 - 299.999: cargas em massa esta semana

Políticas específicos do aplicativo

- 301.000 - 301.999: exceções às seguintes políticas gerais específicas para o aplicativo:

  Por exemplo, server1 nas políticas NY

- 311.000 - 311.999: Políticas que se relacionam à resolução priority1 do Tipo de serviço
- 320.000 - 320.999: Políticas relacionadas a NY
- 331.000 - 331.999: Políticas relacionadas a Lisle

Políticas específicas para a tecnologia

- 410.000 - 410.999: Políticas relacionadas a servidores.
- 411.000 - 411.999: Políticas relacionadas à rede

Políticas padrão

Você pode usar essas políticas se as políticas anteriores não se aplicarem ao seu ambiente.

900.000 - 999.999: Políticas padrão, como todas as atualizações a atributos gerenciados (Qualquer atributo gerenciado) devem ter uma especificação de mudança.

Considerações sobre o Multi-Tenancy

Considere as seguintes informações ao usar o CACF em um ambiente de multilocação:

- Atributos gerenciados, políticas de verificação, Requisições de mudança e especificações de mudança são com titulares.
- Até sua hierarquia, os Inquilinos podem exibir todos os objetos de CACF.

  Por exemplo, se um inquilino cria um atributo gerenciado, essa ação pode bloquear um inquilino na hierarquia de criar um atributo gerenciado duplicado. A hierarquia exige números de sequência de política exclusivos.
- Para determinar a política que gerencia uma mudança em um atributo, considere apenas políticas da hierarquia do inquilino do objeto (IC).
- Um subinquilino pode criar uma política que substitui o superinquilino, designando uma sequência de números mais baixa para a política local.
- O CACF considera apenas políticas no nível do inquilino e seus pais na hierarquia.
- O CACF não considera o inquilino daquele contato que executa a mudança.

  Observação: as políticas de verificação são específicas para o seu sistema e não variam por usuário ou função.

Funções do CACF e acesso funcional

A tabela a seguir descreve as funções padrão que o CACF usa:

Role/Functional Access	Administração	IC	Incidente/Problema /Solicitação	Requisição de mudança
Administrador	Modificar	Modificar	Modificar	Modificar
Administrador de configuração	Modificar	Modificar	Modificar	Modificar
Analista de configuração	Exibir	Modificar	Modificar	Modificar
Visualizador de configuração	Nenhuma	Exibir	Modificar	Exibir
Gerenciador de mudanças	Exibir	Modificar	Modificar	Modificar
Administrador do Service Desk	Modificar	Modificar	Modificar	Modificar

Role/Functional Access	Administração	IC	Incidente/Problema /Solicitação	Requisição de mudança
Service Desk Manager	Exibir	Modificar	Modificar	Modificar
Administrador do sistema	Modificar	Modificar	Exibir	Exibir
Analista de nível 1	Exibir	Exibir	Modificar	Exibir
Analista de nível 2	Exibir	Modificar	Modificar	Modificar
Gerente de incidentes	Exibir	Exibir	Modificar	Modificar
Gerenciador de problemas	Exibir	Exibir	Modificar	Modificar

Administração

Indica como criar, atualizar e exibir a administração, as políticas e o gerenciamento de atributos do CACF.

IC

Indica como criar, atualizar e exibir dados de atributo e de relacionamento de IC.

Incidente/Problema/Solicitação

Indica a modificação e exibição de ocorrências CACF pendentes, incluindo as mudanças informais e variações de execução incorreta de mudanças.

Requisições de mudança

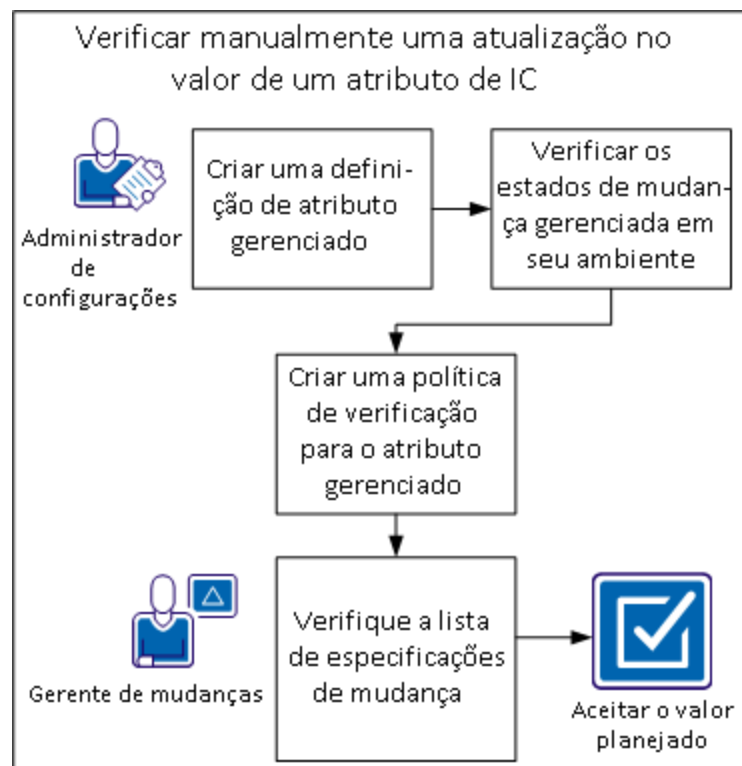
Indica como criar, atualizar e exibir especificações de mudança.

Por exemplo, a função Gerenciador de mudanças pode exibir as políticas CACF e pode gerenciar os atributos, mas não atualiza-los.

Importante: Atualizar acesso à requisição de mudança e seu status determina quem pode editar especificações de mudança. Por exemplo, o Administrador de mudanças oferece esse acesso para o gerenciador de mudanças.

Verificar a Atualização do valor do atributo do IC manualmente

O Administrador de configuração, determina que o ambiente do CA SDM requer uma política de verificação para a Memória instalada (phys_mem). O Administrador de configuração cria uma Definição para o atributo gerenciado com o status *Verificação manual será necessária* porque o CA SDM não possui um MDR para detectar o valor. O Administrador de configuração analisa os estados gerenciados e cria uma política de verificação. O Gerenciador de mudanças exibe uma requisição de mudança que solicita uma atualização do valor da Memória instalada de um IC e essa requisição de mudança exige verificação manual.

O diagrama a seguir explica como um Administrador de configuração determina uma política de verificação e como o Gerenciador de mudanças verifica manualmente a atualização de um valor de atributo de IC:

1. Criar uma Definição de atributo gerenciado (na página 716).
2. Revisar os estados de mudança gerenciada no ambiente (na página 717).
3. Criar uma política de verificação para o atributo gerenciado (na página 717).
4. Revisar a lista de especificações da mudança (na página 719).
5. Aceitar o valor planejado (na página 720).

Criar uma Definição de atributo gerenciado.

O Administrador de configuração cria uma definição para o atributo gerenciado do atributo Memória Instalada (phys_mem).

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da Configuração, Atributos gerenciados.
2. Clique em Criar novo.
3. Digite **phys_mem** como o Nome do atributo.
4. Digite **Memória instalada** como o Rótulo do atributo.
5. Selecione *Verificação manual será necessária* na lista suspensa Status Inicial da verificação.
6. (Opcional) Selecione a opção Diferenciar maiúsculas e minúsculas se deseja aplicar a diferenciação de maiúsculas e minúsculas em comparações de valor planejado de especificações de mudança.

   Padrão: desativado
7. Clique em Salvar.

   O atributo gerenciado é salvo.

Revisar os estados de mudança gerenciada no ambiente.

O Administrador de configuração verifica os estados de mudança gerenciada no ambiente do CA SDM. A verificação da mudança é iniciada quando o status de uma requisição de mudança é alterado para um estado de mudança que o CACF gerencia, como Verificação em andamento.

Observação: o Administrador de configuração pode personalizar qual estado no ciclo de vida da requisição de mudança inicia a verificação. O administrador também pode personalizar quais estados permitem modificar especificações de mudança quando a implementação for iniciada.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da Configuração, Estados de mudança gerenciada.
2. Clique em Implementação em andamento para abrir a página de detalhes de status gerenciado.
3. Revise os detalhes sobre o status gerenciado.

   Por exemplo, você pode decidir tornar o status Implementação em andamento para permitir a edição das especificações de mudança, além de ativar a opção Verificação de mudança ativa. Esse exemplo indica um processo de verificação de mudança ativa e que você pode editar os valores quando a requisição de mudança definir para o status Implementação em andamento.
4. Feche a página.

Criar uma política de verificação para o atributo gerenciado.

A política de verificação especifica a ação do CACF quando um MDR detecta um valor de atributo e tenta atualizar o CMDB com esses dados.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Controle da configuração, Políticas de verificação.
2. Clique em Criar novo para abrir a página de detalhes.
3. Digite **1000** como a Sequência da política.

   Observação: é possível digitar um número inferior ou superior, com base em outras prioridades de política de verificação no seu ambiente.

4. Digite um Nome de política, como **Gerenciamento de RAM** e uma breve descrição da política.
5. Selecione Inserção informal e Atualizações informais em Alinhamento da requisição de mudança.
6. Se você deseja que a política evite que um determinado MDR atualize o atributo Memória instalada (phys_mem), execute as seguintes tarefas:
   - Selecionar memória instalada como o atributo gerenciado.
   - Digite um Padrão de função ou use um asterisco para aplicar a todas as funções.
   - Digite um Padrão de nome do IC ou use um asterisco para aplicar a todos os ICs.
   - Digite um Padrão de classe ou use um asterisco para aplicar a todas as classes.
   - Marque Manter valor do atributo antigo como Comportamento de atualização.

   Observação: se você deseja permitir atualizações a esse atributo por um usuário conectado por meio da interface web, insira **Cliente web** como o Padrão do nome do MDR.
7. Clique em Salvar.
8. Feche a página.

Revisar a lista de especificações da mudança

Uma requisição de mudança com status de RDM deseja alterar o valor do atributo Memória instalada (phys_mem) em um IC chamado server1. O Gerenciador de mudanças define o status de verificação da especificação de mudança para *Verificação Manual será necessária*. O Gerenciador de mudanças pode exibir a Especificação da mudança no CA SDM.

Siga estas etapas:

1. O Gerenciador de mudanças move a requisição de mudança da RDM para a Verificação em andamento.

   Todas as especificações de mudança com o Verificação manual tornam-se Verificação manual ativa.

2. A partir da Requisição de mudança, selecione a guia Especificações de mudança a partir da guia Gerenciamento de configuração.

   A guia destaca todas as especificações de mudança em vermelho para indicar que uma verificação manual é necessária.

   Observação: também é possível ver as especificações de mudança na guia Administração ao clicar em CA CMDB, Configuração do Audit, Especificações de mudança. Além disso, exiba as especificações de mudança a partir de um IC depois de selecionar a guia Especificações de mudança na guia Tickets relacionadas.

3. Pesquisar especificações de mudança com a opção *Requer verificação manual* como o Status da verificação.

   Por exemplo, alterar as especificações da requisição de mudança 21 tem esse status.

4. Pesquisar o valor apropriado dd o atributo Memória Instalada para o IC server1.

   Observação: as especificações de mudança que não passaram na verificação também são exibidas em vermelho para mostrar as especificações de mudança que requerem mais atenção.

Aceitar o valor planejado.

O Gerenciador de mudanças pesquisa o valor de atributo correto para o IC e toma a decisão correta sobre a requisição de mudança.

Siga estas etapas:

1. Abra a Especificação da mudança para exibir a página de detalhes.
2. Você procura o atributo Memória instalada (phys_mem) específico para o IC e confirma o valor planejado.
3. Verifique se a requisição de mudança da especificação de mudança está no estado Verificação em andamento.
4. Clique em Aceitar valor planejado.

   O Status de verificação muda para Valor planejado aceito.

   Observação: depois de clicar em Aceitar Valor planejado, o IC é atualizado com o valor planejado automaticamente.

Você concluiu com êxito a verificação manual do valor de atributo gerenciado.

Exemplo: Permitir Atualizações informais somente a partir de um Local específico

Nesse exemplo, os ICs de servidor no escritório de Nova Iorque precisam de reparo. O fornecedor que faz os reparos nos servidores também se encontra em Nova York. O Asset Manager requer que sua organização envie todos os servidores defeituosos para Nova York. O Administrador de configuração deseja permitir atualizações informais em ICs quando o hardware chegar em Nova York. O Administrador de configuração cria um uma política de verificação para o atributo do Fornecedor de manutenção para que um Analista do Service Desk em Nova Iorque possa verificar se o fornecedor recebe os servidores.

Siga estas etapas:

1. Criar o seguinte atributo gerenciado:
   - Digite **vendor_repair** como o Nome do atributo.
   - Selecione a verificação pendente a partir da lista suspensa Status inicial.
   - Digite **Manutenção** como o rótulo e descrição para obter detalhes sobre o atributo gerenciado.
2. Crie o seguinte status de mudança gerenciada:
   - Digite **Retido pelo fornecedor** como status da requisição de mudança.
   - Ative a opção Verificação de mudança ativa.

3. Criar a seguinte política de verificação:
   - Selecione Inserção informal e Atualização informal como alinhamentos da requisição de mudança.
   - Digite um número de sequência para a política.

     Por exemplo, digite **201.**
   - Digite **server*** como o nome do Padrão de IC.
   - Digite **Servidor** como o Padrão de classe.
   - Digite **Nova York** como o padrão de Local.
   - Selecione Permitir atualização do atributo na lista suspensa Comportamento de atualização.
4. O Analista do Service Desk cria uma requisição de mudança e especificações de mudança para os ICs do servidor e especifica Nova York para o local.
5. O Analista do Service Desk define o status da requisição de mudança para Retido pelo fornecedor.
6. O Analista do Service Desk atualiza o local para os ICs do servidor como Nova York.

   Por exemplo, os servidores com defeito do escritório de Chicago são enviados para Nova York e Analista do Service Desk verifica se os servidores chegaram em Nova York.
7. O Analista do Service Desk digita as informações do fornecedor no IC.

   A requisição de mudança é fechada depois que todos os locais de IC são definidos para Nova Iorque e todas as especificações de mudança são verificadas.

Exemplo: Atualizar laptops na organização

Neste exemplo, o Asset Manager deseja atualizar todos os laptops do Windows XP para o Windows 7 na organização. O Administrador de configuração cria uma política de verificação para o atributo Versão do produto, a fim de filtrar todos os laptops com o sistema operacional Windows XP. O Administrador de configuração cria uma definição de atributo gerenciado com o status *Usar valor detectado*, revisa os Estados gerenciados e cria uma política de verificação. o CA SDM recebe atualizações para o CMDB do CA Configuration Automation dos laptops que precisam de uma atualização do sistema operacional e a equipe de Gerenciamento de ativos conclui a atualização.

Siga estas etapas:

1. Criar o seguinte atributo gerenciado:
   - Digite **product_version** como o Nome do atributo.
   - Digite a **Versão do produto**, como o Rótulo do atributo.
   - Selecione Usar valor detectado da lista suspensa Status inicial.
   - Digite um rótulo e descrição para os detalhes sobre o atributo gerenciado.
2. Criar a seguinte política de verificação:
   - Digite uma sequência com base em outras políticas da organização.

     Por exemplo, digite **101.**
   - Digite **Windows* XP*** como o Padrão de Nome do IC.
   - Digite **Workstation** como Padrão de classe.
   - (Opcional) Digite um Padrão de Local se deseja associar a política com um escritório específico da organização.
   - Selecione Permitir atualizar somente se corresponder à especificação da mudança a partir da lista suspensa Atualizar comportamento.
   - Selecione Sim na lista suspensa Criar incidente.
3. Crie uma requisição de mudança e especificações de mudança que especifiquem o Windows 7 para o atributo gerenciado Versão do produto para cada um dos ICs de laptop.
4. Mova a requisição de mudança para o status Implementação em andamento e aguarde até sua equipe de Gerenciamento de ativos inicie o processo de atualização.

5. Quando as implementações forem concluídas, mova a requisição de mudança para Verificação em andamento.

   O CA Configuration Automation detecta as informações de laptop e importa os dados para o CMDB.

6. Exibir a lista aberta de Incidentes de CACF para obter quaisquer variações que o CACF tiver detectado.

7. Selecione um dos incidentes e revise os detalhes sobre o laptop que o CA Configuration Automation detectou.

8. Clique em Criar requisição de mudança e associe o IC ao ticket; especifique as especificações de mudança da Versão do produto em relação às mudanças pendentes.

   Aguarde até que a detecção verifique se todas as mudanças restantes foram concluídas.

9. Repita as Etapas 6 a 8, conforme necessário, para quaisquer novos incidentes que CACF criar.

Exemplo: Bloquear requisições de mudança não verificados

Nesse exemplo, o Administrador de configuração deseja permitir somente uma atualização de IC de uma requisição de mudança correspondente. Somente ICs na classe de Servidores localizados em NY são atualizados em relação às requisições de mudança. Qualquer variação cria um incidente.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Digite **NY** como o Padrão de local.
   d. Digite **Servidor** como Padrão de classe.
   e. Selecione Permitir Atualização apenas se a especificação da mudança corresponder como Comportamento de atualização.
   f. Selecione Sim na lista suspensa Criar incidente.
3. Salve a política.

Exemplo: permitir uma Atualização de IC se não houver requisição de mudança correspondente

Nesse exemplo, o Administrador de configuração deseja permitir atualizações de todos os ICs de teste chamados test*, mesmo se não houver nenhuma requisição de mudança correspondente. Essa política aceita atualizações de todos os usuários em funções administrativas.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Digite **test*** como o Padrão de nome do IC.
   d. Digite **Administrador*** como Padrão de função.
   e. Selecione Permitir atualização do atributo como Comportamento de atualização.
3. Salve a política.
4. Um usuário com função administrativa cria uma especificação de mudança de um IC chamado test5.

   O IC atualiza com êxito.

Exemplo: adiar todas as atualizações do CA Configuration Automation para a TWA

Nesse exemplo, o Administrador de configuração deseja adiar todas as atualizações de ICs do CA Configuration Automation na TWA. Essa política não atualiza o IC no CMDB e grava os dados de todas as mudanças informais na TWA para avaliação posterior.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Selecione Inserção informal e Atualização informal como Alinhamento da requisição de mudança.

d. Digite o **CCA** como o Padrão de classe do MDR.

e. Selecione Cancelar sempre a transação toda como Comportamento de atualização.

f. Selecione Sempre para Gravar os dados na opção TWA.

3. Salve a política.

Exemplo: Registrar somente os Resultados da política como um teste

Nesse exemplo, o Administrador de configuração deseja testar uma nova política antes de implementa-la no ambiente CMDB. A opção Somente log permite à CACF gravar os possíveis impactos do IC da política no arquivo de log padrão.

Siga estas etapas:

1. Crie uma política de verificação.
2. Preencha as informações de alinhamento, filtros e ação.
3. Selecione a opção Modo de log somente.
4. Salve a política.
5. Exibir o arquivo padrão de log, depois de executar atualizações de IC que correspondam às especificações de política e os critérios de filtro para simular a execução da política.

Exemplo: Rejeitar uma atualização de IC

Nesse exemplo, o Administrador de configuração deseja rejeitar atualizações de um MDR chamado Cohesion para o atributo endereço IP (alarm_id) apenas. Essa política não atualizará o endereço de IP do IC no CMDB enquanto ele puder atualizar outros atributos. O CACF grava todos os atributos na TWA para avaliação.

Siga estas etapas:

1. Adicionar Endereço IP (alarm_id) na lista de atributos gerenciados.
2. Crie uma política de verificação.
3. Conclua as seguintes etapas:

   a. Digite um número de sequência.

   b. Selecionar o endereço IP como o atributo gerenciado.

c. Selecione Inserção informal e Atualização informal como Alinhamento da requisição de mudança.
   d. Digite **Cohesion** como padrão de MDR.
   e. Marque Manter valor do atributo antigo como Comportamento de atualização.
   f. Selecione Sempre para Gravar os dados na opção TWA.
4. Salve a política.

Exemplo: Permitir requisições de mudança criadas sem especificações

Nesse exemplo, o Administrador de configuração deseja confiar nas requisições de mudança que os usuários criaram sem as especificações. Essa política pressupõe que o texto do IC texto descreve todas as mudanças com precisão e permite a atualização do IC.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Selecione Requisições de mudança sem especificações como o alinhamento.
   d. Selecione Permitir atualização do atributo como Comportamento de atualização.
3. Salve a política.

Exemplo: Não permitir requisições de mudança criadas sem especificações

Nesse exemplo, o Administrador de configuração *não* deseja confiar nas requisições de mudança que os usuários criaram sem as especificações. Essa política ignora requisições de mudança sem especificações e cria incidentes.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Selecione Requisições de mudança sem especificações como o alinhamento.
   d. Selecione Cancelar sempre a transação toda como Comportamento de atualização.
   e. Selecione Sim na lista suspensa Criar incidente e, em seguida, selecione um modelo de Incidente.
3. Salve a política.

Exemplo: permitir inserções informais de fontes selecionadas

Nesse exemplo, o Administrador de configuração deseja permitir novos ICs de fontes selecionadas. Os z/OS MDRs podem criar ICs sem a necessidade de uma requisição de mudança.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione Qualquer atributo gerenciado como o Atributo gerenciado.
   c. Selecione Inserção informal como alinhamento.
   d. Digite o **z/OS** como o Padrão de classe do MDR.
   e. Selecione Permitir atualização do atributo como Comportamento de atualização.
3. Salve a política.

Exemplo: permitir uma atualização informal de um IC que não seja de produção

Nesse exemplo, o Administrador de configuração deseja permitir atualizações ao atributo de endereço IP do Spectrum MDR, mas o nome não pode começar com *PROD*.

Siga estas etapas:

1. Crie uma política de verificação.
2. Conclua as seguintes etapas:
   a. Digite um número de sequência.
   b. Selecione o endereço IP(alarm_id) como o atributo gerenciado.
   c. Selecione Atualização informal como alinhamento.
   d. Digite **!PROD*** como o Padrão de nome do IC.
   e. Digite **Spectrum** como o Padrão de classe do MDR.
   f. Selecione Permitir atualização do atributo como Comportamento de atualização.
3. Salve a política.

Capítulo 15: Administração de MDRs

Este capítulo descreve como definir MDRs, importar dados, mapear ICs à sua origem, definir parâmetros de lançamento, lançar de volta ao MDR de origem e usar MDRs para mapear e exibir informações de ICs federados.

Esta seção contém os seguintes tópicos:

O que é um MDR? (na página 729)
MDR Launcher (na página 731)
Definir um URL para iniciar um MDR (na página 732)
Configurar um MDR como provedor do CA APM (na página 734)
Execução em contexto do CA CMDB para o CA APM (na página 735)
Propriedades de ICs que oferecem suporte à federação do MDR (na página 735)
MDRs do CA Cohesion ACM (na página 738)
Usando o GRLoader (na página 743)
Convenções e restrições de nomenclatura de ICs (na página 743)
Convenção de nomenclatura de system_name (na página 745)
Usando o visualizador do CMDBf (na página 746)
Como atualizar arquivos de metadados para mapeamento do CMDBf (na página 747)

O que é um MDR?

A CMDBf (Configuration Management Database Federation - Federação de Banco de Dados de Gerenciamento de Configuração), um grupo de trabalho composto por representantes da CA, IBM, HP, Microsoft e outras empresas, define um MDR (Repositório de Dados de Gerenciamento) como tudo que coleta informações sobre ICs (Itens de configuração).

Para criar o relacionamento entre um MDR e seus ICs ao implementar o MDR Launcher, faça o seguinte:

1. Defina o MDR.
2. Defina os ICs que fazem referência ao MDR.

   Não é possível ter um IC que faça referência a um MDR inexistente, mas é possível definir um IC sem definir a associação com um MDR. Você pode adicionar as informações do MDR durante uma atualização ou edição para aproveitar ao máximo os recursos do MDR Launcher.

O mesmo IC pode ser detectado por vários MDRs. Depois que o IC é detectado, cada MDR tenta administrar esse IC. Um MDR pode fazer o seguinte:

- Detectar atributos detalhados sobre o IC.
- Tentar modificar o estado do IC.

Exemplo: um IC detectado por vários MDRs

Um IC é detectado tanto pelo software de gerenciamento de rede quanto por um pacote de software de gerenciamento de ativos.

- O software de gerenciamento de rede mantém informações sobre a configuração e a topologia da rede.
- O software de gerenciamento de ativos contém informações sobre custo, depreciação, licenciamento e contratos de manutenção para esse determinado IC.

Classes e nomes de MDRs

Uma empresa de TI pode incluir muitos MDRs. Cada MDR tem um identificador chamado *Nome do MDR (mdr_name*). Como é comum um MDR usar o nome de servidor host como o *mdr_name* (para permitir que vários MDRs residam no mesmo servidor host), uma *classe de MDR* (*mdr_class*) é acrescentada ao *mdr_name* para identificar cada MDR de forma exclusiva.

O CA Cohesion ACM é uma ferramenta de detecção corporativa que se integra perfeitamente ao CA CMDB. Cada MDR do CA Cohesion ACM definido para o CA CMDB deve ter uma *mdr_class* do **Cohesion**.

Observação: para obter mais informações sobre o CA Cohesion ACM, consulte a ajuda online do CA Cohesion ACM. Para a integração CA Cohesion ACM/CA CMDB, consulte o *Guia de Implementação do CA Cohesion ACM*.

Como o MDR complementa o CA SDM?

Um MDR geralmente contém informações mais detalhadas sobe o IC do que o CA CMDB. No entanto, um único MDR geralmente não tem conhecimento da existência de outros MDRs nem se concentra nos relacionamentos que um IC específico pode ter com outros ICs, especialmente se eles estiverem contidos em outros MDRs. O CA CMDB é especificamente adequado para gerenciar esse tipo de ambiente, pois se concentra no gerenciamento de ICs independentemente de sua origem de MDR.

O CA CMDB não se destina a armazenar todos os atributos de todos os ICs. Em vez disso, ele é usado para consolidar os atributos mais importantes que devem ser gerenciados centralmente. Os atributos sob o controle do gerenciamento de mudanças são excelentes candidatos para inclusão no CMDB. Atributos não gerenciados pelo CA CMDB podem ser acessados usando o recurso MDR Launcher. Adicionalmente, o CA CMDB fornece o visualizador de CMDBf, que permite comparação lado a lado de atributos de IC através de vários CMDBs e MDRs.

Definição de MDR para o CA SDM

A guia Administração permite definir um MDR para o CA CMDB.

Antes de importar um IC para um MDR, esse MDR deve ser definido. As tentativas de importar um IC federado para um MDR inexistente não serão bem-sucedidas.

Observação: Para obter instruções sobre como definir um MDR, consulte o *Guia de Implementação do*.

MDR Launcher

O MDR Launcher é uma ferramenta de integração aberta que permite exibir dados de praticamente qualquer MDR usando uma página da Web sem necessidade de codificação. O MDR Launcher permite que qualquer pessoa que esteja exibindo um IC possa obter detalhes adicionais sobre o IC e assumir o controle sobre ele (se o MDR oferecer suporte a esse controle).

Alguns usos do MDR Launcher são os seguintes:

- Na página de detalhes Hardware.Servidor, inicie o CA Cohesion ACM para verificar uma mudança.
- Nos detalhes de um IC de Ar condicionado, inicie a página web de um fornecedor para obter informações de diagnóstico e o relatório de incidentes.
- Em um IC de Contrato, inicie um sistema de gerenciamento de contratos para consultar os detalhes do contrato.
- Em um IC de SLA, inicie o Serviço CA para revisar os acordos de nível de serviço antes de fazer uma mudança.
- Em um IC de Servidor, inicie o CA Remote Control para assumir o controle do servidor a fim de diagnosticar e corrigir um problema.

Definir um URL para iniciar um MDR

O CA CMDB usa um URL para iniciar uma sessão do navegador da web com o MDR de origem para operar o MDR Launcher. Você pode definir o URL usado pelo CA CMDB.

Para definir um URL para um MDR

1. Clique na guia Administração.
2. Na seção esquerda, abra o CA CMDB, árvore de Gerenciamento do MDR.
3. Clique na Lista de MDR.

   A página Lista de repositórios de dados de gerenciamento (MDR) é exibida.
4. Clique em um MDR existente (ou crie e salve um novo).

   A página Definição do provedor do MDR aparece.
5. Clique em Editar.

   A página Atualizar definição do MDR aparece.
6. Preencha os seguintes parâmetros:

   Nome do host

   Especifica o endereço de rede ou nome DNS do servidor web que fornece páginas web ao MDR.

   Porta

   Especifica o número da porta usada pelo servidor web do nome do host.

Caminho

Especifica o caminho até a página web, incluindo a própria página.

Parâmetros

Especifica todos os parâmetros usados para identificar o IC desejado para o MDR. O CA CMDB publica essa informação no MDR.

ID do usuário

Especifica a ID de usuário, se uma ID de usuário comum tiver permissão de acessar o MDR.

Segredo compartilhado

Especifica informações a serem compartilhadas entre o CA CMDB e o MDR. Para MDRs do CA Cohesion, o valor especificado aqui deve corresponder ao valor especificado no arquivo de propriedades do CA Cohesion, para o valor com.cendura.security.oneclickauth.secret.

Namespace do CMDBf

Especifica o federated_asset_id que é passado para a consulta como uma ID local. Para o CA CMDB, o valor é http://cmdb.ca.com/r1.

CMDBf Timeout

(Opcional) Especifica o limite de tempo para a consulta do ponto de extremidade do CMDBf. O padrão é 10 (dez) segundos.

Ponto de extremidade do CMDBf

Especifica o ponto de extremidade do Serviço de consulta para o MDR. Obrigatório para o Visualizador do CMDBf e recuperando os dados MDR atualizados. Se você usar o CA CMDB como um provedor do MDR, o valor será http://cmdb_hostname:cmdb_port/axis/services/QueryPort.

Salve a definição.

O URL é definido.

Observação: além disso, o URL pode conter variáveis de substituição para qualificar adicionalmente o IC para o MDR. Para obter mais informações, consulte o *Guia de Implementação*.

Configurar um MDR como provedor do CA APM

É possível configurar um MDR para ser o provedor do CA APM.

Siga estas etapas:

1. Na guia Administração, clique em CA CMDB, Gerenciamento do MDR, Lista do MDR.
2. Clique em Criar para especificar o MDR do CA APM.

   A página de definição de provedor do MDR aparece.
3. Insira as seguintes informações obrigatórias para o provedor do MDR:
   - Nome do botão — Especifique APM ou qualquer outro nome de botão válido. Recomendamos usar o nome de botão APM.
   - Nome do MDR: especifique APM para CA Asset Portfolio Management r11.3.4 ou ITAM para CA APM r12.6
   - Classe do MDR — Especifique GLOBAL.
   - Nome do host — Especifique o nome do servidor do CA APM que usa o endereço de rede ou o Nome DNS do servidor web do CA APM.
   - URL para execução em contexto — Especifique http://{hostname}:{port}/{path}?{parameters}. Não deve ser alterado.

   O formulário Provedor do MDR preenche automaticamente o caminho e os valores do parâmetro com as informações necessárias para execução em contexto do CA APM.
4. Clique em Salvar.

   O provedor do MDR do CA APM é configurado.

   Observação: para obter mais informações sobre o MDR Launcher, consulte o *Guia de Implementação*.

Execução em contexto do CA CMDB para o CA APM

O recurso MDR Launcher do CA CMDB oferece suporte à execução em contexto para o CA APM quando o CA APM e o CA CMDB compartilham o mesmo MDB. A UI do CA CMDB fornece um botão de execução em contexto na guia Atributos do formulário Detalhes do IC quando o usuário cria uma definição de provedor do MDR especial do CA APM.

A definição de MDR do CA APM tem todos os recursos de um MDR tradicional. O recurso Controle de versão do CA CMDB também oferece suporte à execução em contexto diretamente de uma entrada de log de atributo associada a cada mudança do CA APM.

Importante: Ao contrário de outros MDRs, o MDR do CA APM é automaticamente associado a cada IC ou ativo. A classe GLOBAL do MDR e o nome APM do MDR são usados para identificar o MDR do CA Asset Portfolio Management r11.3.4. A classe MDR de nome GLOBAL e de MDR do ITAM são usadas para identificar o MDR do CA APM r12.6. O uso do MDR do CA APM é totalmente compatível com outros MDRs, ainda que para o mesmo IC.

Propriedades de ICs que oferecem suporte à federação do MDR

As propriedades de item de configuração (atributos) identificam ativos para fins de federação de MDR.

ID do ativo federado

As pessoas são conhecidas para diferentes organizações por identificadores distintos. Você pode ser conhecido pelos seguintes identificadores:

- Um apelido exclusivo para seus amigos próximos
- Carteira de motorista (identificação exclusiva associada a você)
- Identificação de serviço militar (por exemplo, um cartão de serviço seletivo)
- Número de seguro-saúde
- CPF

Cada um desses identificadores exclusivos se refere a você. No entanto, os identificadores são válidos apenas quando usados para identificá-lo para o repositório adequado.

Da mesma forma, um IC pode ter vários identificadores para associá-lo a seus MDRs de origem. Cada IC é reconhecido por um MDR apenas por um único identificador. Chamamos esse identificador de *ID do ativo federado*. O processo de associação de um IC a um ou mais MDRs é chamado de *mapeamento do IC*.

O mapeamento ocorre quando os ICs são carregados no MDB de uma destas duas formas:

- Definição do mapeamento do IC usando a interface de usuário Administração
- Carregamento de ICs usando o utilitário GRLoader

Nome do MDR

O nome do MDR identifica o MDR para o CA CMDB ao exportar dados usando XML e GRLoader. O MDR normalmente possui sua própria convenção de nomenclatura para se identificar: uma combinação de nome do servidor host com um nome ou número de instância de identificação. Como existe apenas um MDR em um determinado host, o nome do MDR é frequentemente definido como o nome do servidor host. **Obrigatório para o Visualizador do CMDBf.**

Importante: O nome do MDR da release CA Asset Portfolio Management 11.3.4 é APM e o nome do MDR do CA APM r12.6 é ITAM. Ambos os produtos são suportados, no entanto, recomendamos que você verifique a disponibilidade do produto em supportconnect.ca.com antes de implementar os produtos.

Classe do MDR

A classe do MDR é definida pelo cliente para agrupar MDRs.

Observação: Uma classe MDR de CMDBf é necessária para exibição do CMDBf.

Importante: O nome do MDR junto com a Classe do MDR devem ser exclusivos na empresa.

Definição de MDRs com instalação do CA Cohesion ACM

Os MDRs do CA Cohesion ACM têm os seguintes requisitos:

- O mdr_name especificado na definição do MDR no servidor do CA CMDB deve corresponder exatamente ao valor do atributo com.cendura.installation.name no arquivo cendura.properties no servidor de destino do CA Cohesion ACM.
- Os MDRs do CA Cohesion ACM devem ter uma classe de MDR do Cohesion.
- O MDR deve especificar o nome do host e o número da porta do servidor do CA Cohesion ACM.

Para executar o MDR Launcher, edite a seguinte parte do arquivo cendura.properties:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=shared_secret
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=userid
```

Importante: O segredo especificado no arquivo cendura.properties deve corresponder ao *segredo compartilhado* na definição do MDR.

O MDR Launcher efetua logon com a *ID de usuário* especificada no arquivo de propriedades e herda seus atributos de segurança. Para usar funcionalidades como Atualizar para atributos de ICs, verifique se o usuário tem privilégios suficientes.

Observação: para obter mais informações sobre como criar um usuário e definir opções de segurança para esse usuário, e para personalizar o arquivo de propriedades, consulte o *Guia de Implementação do CA Cohesion ACM.*

MDRs do CA Cohesion ACM

MDRs do CA Cohesion ACM devem ser definidos antes da importação de dados de um servidor do CA Cohesion ACM. Um MDR do CA Cohesion ACM deve especificar uma classe de MDR do Cohesion.

Exemplo: definição do MDR Cohesion1

Na seguinte definição do MDR Cohesion1, o XML especifica o nome do MDR como cohesion_server e a Classe do MDR como Cohesion. Esses valores são obrigatórios para que os ICs sejam importados.

Nome do botão

Cohesion1

Nome do MDR

cohesion_server

Classe do MDR

Cohesion

Ativo?

Ativo

Proprietário

CMDBAdmin

Descrição

Servidor do CA Cohesion ACM em Chicago

Nome do host

cohesion_server

Porta

8090

Caminho

CAisd/html/cmdb_cohesion.html

Parâmetros

hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}

id do usuário

cohesion_userid

Segredo compartilhado

Chicago01

URL para execução no contexto

http://cmdb_hostname:8080/{path}?{parameters}

Além disso, como se trata de um servidor Cendura, os valores acima devem corresponder aos valores no arquivo cendura.properties nesse servidor, como mostra o seguinte exemplo:

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

É possível modificar a sintaxe do URL para lidar com requisitos especiais.

Como associar um MDR a um IC manualmente

É possível associar manualmente MDRs a um IC usando o recurso Mapeamento dos ICs federados encontrado na guia Administração do CA CMDB, em Gerenciamento do MDR da árvore.

Antes de associar um IC a um MDR, faça o seguinte:

1. Criar a definição do MDR (caso não exista).
2. Criar a definição do IC (caso não exista).
3. Identificar a ID do ativo federado do IC que deseja conectar ao MDR. Essa ID é específica de cada MDR, portanto, está além do escopo deste documento.

   Observação: para identificar a ID do ativo federado, consulte a documentação do MDR.

Importação automática do CA Cohesion

É possível importar ICs diretamente do CA Cohesion ACM executando um relatório do CA Cohesion ACM que especifique o nome do host, a porta, a ID e a senha do usuário para um servidor do CA CMDB. Se o MDR estiver definido no CA CMDB, o CA Cohesion gerará automaticamente o XML para criar ICs e relacionamentos, junto com as informações necessárias para executar o MDR Launcher em um IC. O relatório importa automaticamente os ICs para o CA CMDB.

Observação: para obter mais informações sobre como exportar ICs do CA Cohesion ACM, consulte a ajuda online disponível na guia Relatórios, Modelos de relatório.

IC para mapeamento do MDR

Como cada MDR usa um federated_asset_id para identificar um IC, um IC pode ser relacionado a vários MDRs. Um federated_asset_id não tem que ser exclusivo entre os MDRs, mas um federated_asset_id deve ser exclusivo em um MDR. Cada MDR deve ter uma classe de MDR e um nome de MDR exclusivos.

Importante: sempre que um IC ou um provedor de MDR é tornado inativo, todos os mapeamentos de ICs federados associados ao IC ou provedor de MDR também são tornados inativos.

Após criar uma definição de Provedor de dados do MDR, faça o seguinte:

1. No CMDB, crie um IC que faça referência a um MDR.
2. Verifique se a definição do MDR funciona.

   Como você pode iniciar apenas no contexto de um IC, não é possível testar diretamente a partir da definição do MDR, que não possui contexto de IC.

Você pode exibir a Lista de mapeamentos de ICs federados na guia Administração, no nó Mapeamento de ICs federados.

Para exibir o IC em um contexto de MDR específico, clique no botão MDR Launcher.

O MDR de destino é iniciado no contexto do IC aberto.

Exemplo: mapeamento de ICs

1. Clique na guia Administração.
2. Navegue até Gerenciamento do MDR, Mapeamento dos ICs federados.

   A Lista de mapeamentos de ICs federados é exibida.
3. Insira server1 no campo Nome do IC.

   As seguintes colunas mostram os valores:

   ID do ativo federado

      1000234

      1000235

   Nome do CI

      server1

      server1

   Provedor do MDR

      Cohesion1

      Cohesion2

   Ativo

      Ativo

      Ativo

   O Provedor do MDR do Cohesion1 sabe da existência do server1, e o Provedor do MDR do Cohesion2 também sabe da existência do server1. O exemplo mostra que cada um deles atribuiu de forma independente uma ID exclusiva ao servidor.
4. Clique no nome do IC server1.

   A página Detalhes do item de configuração do server1 aparece, incluindo botões de execução, que podem ser chamados de Cohesion1 e Cohesion2.
5. Clique em um dos botões de execução Provedor de MDR.

   São exibidos detalhes adicionais sobre o IC.

Administração da definição de MDR

Administrar definições de MDR é um processo flexível. Você pode modificar os parâmetros em uma definição de MDR mesmo quando ICs fazem referência a ele. Por exemplo, nome do botão, nome do host, ID do usuário, segredo compartilhado e outras opções podem ser modificadas após o MDR ser definido e os ICs carregados.

Relatório do CA Cohesion ACM

O CA Cohesion ACM fornece um recurso para programar relatórios recorrentes. É possível usar esse recurso para simplificar o processo de manter o CMDB sincronizado com os dados no MDR do CA Cohesion ACM. Erros comuns, como senha inválida (devido à mudança ou expiração da senha), podem impedir a importação bem-sucedida de dados. Para ser notificado de qualquer erro que possa ocorrer durante a execução de dados em segundo plano na importação de dados, ative a opção Notificação no relatório Exportação do CA CMDB no CA Cohesion ACM. Um email será enviado para você informando quando um erro de importação ocorrer. Se o relatório do Cohesion for executado em segundo plano como uma tarefa programada, recomendamos ativar a opção Notificação.

Observação: para obter informações sobre como programar regularmente a execução do relatório de exportação do CA CMDB, consulte o *Guia do Produto CA Cohesion ACM*.

Usando o GRLoader

Ao usar o GRLoader para carregar um IC, você deve preencher os seguintes campos no XML para que o MDR Launcher opere:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

Os valores fornecidos para <mdr_name> e <mdr_class> no XML devem corresponder exatamente aos valores fornecidos na definição do MDR.

Importante: O nome e a classe do MDR devem ser definidos usando a interface de administração para que os ICs que fazem referência ao MDR possam ser importados. Se o MDR especificado no XML não estiver definido, o IC não será importado.

O GRLoader oferece suporte à importação de ICs e relacionamentos de ICs a partir de planilhas em formato XLS e XLSX. Para carregar os dados de IC no CA SDM, você deve formatar os dados de origem para XML ou planilhas do Microsoft Excel.

Observação: para obter mais informações sobre como usar o GRLoader para carregar dados da planilha, consulte o *Guia de Referência Técnica do CA CMDB*.

Convenções e restrições de nomenclatura de ICs

ICs possuem as seguintes convenções e restrições de nomenclatura:

- Nome do CI

  Esse é o nome comum ou de exibição usado em todas as listas de ICs. O comprimento total do nome não deve exceder 255 caracteres. O nome do IC não precisa ser exclusivo, mas recomendamos que ele seja globalmente exclusivo. Além disso, para situações em que o nome é determinado por um MDR, recomendamos que os administradores do MDR enfatizem a legibilidade humana ao preencher este campo.

- ICs de software

  Para software de terceiros, siga a mesma convenção de nomenclatura para qualquer IC, como os nomes que você cria manualmente usando a guia Administração. Corresponder convenções de nomenclatura permite que ICs detectados pelo CA Cohesion ACM se reconciliem com os criados manualmente. Se essa convenção não for seguida, vários ICs podem ser criados mesmo quando houver apenas uma instância de software.

- Uso do atributo systemname

  O atributo systemname associa exclusivamente um *único* IC a um nome de host específico.

  Se vários ICs são importados e especificarem o mesmo systemname que um IC existente, a reconciliação ajuda a garantir que o resultado é somente um IC.

Exemplo:

As seguintes linhas de saída mostram a criação de um IC de servidor (provedor), um IC de software (dependente) e um relacionamento de *execução* entre eles. O relacionamento resultante representa um servidor que executa o software Apache.

```
CI:  Name: Server1     Class: Server   Systemname: Server1
CI:  Name: Apache1   ON Server1      Class: Software
Relationship:  Server1 runs Apache1   ON Server1
```

Convenção de nomenclatura de system_name

Recomendamos os seguintes padrões de nomenclatura para ICs de software e todos os MDRs, de modo que outros MDRs possam se integrar bem com o CA Cohesion ACM e entre si, e que os ICs se reconciliem adequadamente. O CA Cohesion ACM segue os mesmos padrões.

System_name

Identifica um IC de software exclusivamente. Ao definir um relacionamento que envolva um IC de software, especifique o mesmo system_name da definição desse IC. Se várias instâncias da mesma versão do mesmo software forem instaladas no diretório no mesmo nome de host, modifique system_name para impor exclusividade. O comprimento total de system_name não deve exceder 255 caracteres. Pode ocorrer corrupção de dados se essa restrição for violada.

System_name deve ser um identificador exclusivo dessa instância do software em um único host.

Use a seguinte sintaxe:

```
hostname | softwarename | version | business-application
```

barra vertical (|)

Separa os diversos campos na concatenação da sintaxe para permitir ao usuário usar o recurso de pesquisa.

nome dohost

Especifica o nome do host que contém o software.

softwarename

Especifica um nome comum para o software.

version

Especifica o número da versão do software, se disponível.

business-application

Especifica um identificador exclusivo para essa instância do software no *nome do host*. Se a instância do software estiver associada a um aplicativo ou serviço comercial, o nome desse serviço será o qualificador. Quando você não puder determinar *business-application*, use o guia de instalação para identificar o software. Se o comprimento total desse campo exceder 255 caracteres, reticências (...) devem ser usadas para diminuir o comprimento do campo para no máximo 255 caracteres.

Exemplos: Usar o recurso de pesquisa de UI

É possível usar o recurso de pesquisa de UI para pesquisar ICs de software, como mostram os seguintes exemplos:

Caso de uso	Nome	System_name
Localizar todos os ICs de software no host	xxx	Xxx%
Localizar todas as instâncias do software	yyy	yyy%
Localizar todas as instâncias do software	yyy versão 123.0	yyy% %|%|123.0%

Na lista de resultados retornados na pesquisa acima, o usuário vê apenas o campo Nome.

```
mac_address     Null.  - Inappropriate for software
asset_num       Null   - Inappropriate for software
serial_number   Null   - Inappropriate for software
dns_name        Null   - Inappropriate for software
```

Usando o visualizador do CMDBf

O CA SDM fornece o Visualizador do CMDBf para exibir os resultados da federação do IC através de MDRs. A partir da página CI Detail (ou do menu ao clicar com o botão direito do mouse no IC na Lista de ICs), clique no Visualizador do CMDBf para visualizar os atributos do IC de MDRs e CMDBs federados em paralelo. Na página Federated View, é possível clicar em Recuperar para atualizar as informações de qualquer um dos MDRs federados. Para melhorar a legibilidade, os arquivos de metadados do CA CMDB podem reconciliar os nomes de atributo do MDR e do CA CMDB.

Observação: esse recurso requer MDRs que ofereçam suporte a Consulta. Você configura MDR CMDBf Endpoints para exibir seus resultados em Federated View. Para obter mais informações, consulte o *Guia de Implementação*.

Se o IC não tem nenhum dado federado, o visualizador exibe somente atributos do CA CMDB.

Como atualizar arquivos de metadados para mapeamento do CMDBf

Para melhorar a legibilidade das comparações de atributo, é possível usar os arquivos de metadados do CA CMDB para realizar a tradução entre os nomes de atributo do MDR e os do CA CMDB. Para qualquer atributo MDR que não tenha um mapeamento do CA CMDB, a Federated View exibe o nome do atributo enviado pelo MDR. Os metadados podem ser definidos para os provedores de dados CMDBf para fazer o seguinte:

- Exibir valores de atributos do MDR usando os nomes de atributos do CA CMDB
- Evitar que os atributos MDR do fornecedor sejam exibidos na Federated View
- Definir os atributos MDR do fornecedor que não possuem equivalentes do CA CMDB.

Defina os metadados usando o arquivo cmdb_metadata_federation_viewer_site_attr.htmpl. Esse arquivo contém instruções sobre como atualizar o arquivo. Os metadados podem ser aplicados a todas as famílias do CMDB (atributos comuns) ou atributos específicos da família.

Para mapear os nomes de atributo de MDR externos para os rótulos do CA CMDB, atualize o respectivo formulário cmdb_metadata_*extensiontable*.htmpl usando os seguintes campos na macro cmdbmetadata:

- mdr_attr - o nome do atributo MDR a ser traduzido.
- mdr_name - o nome do MDR sendo traduzido. As expressões comuns são suportadas.

Exemplo: mapeamento de atributos

As três instruções de metadados a seguir definem o metadado que equaciona o atributo "phys_mem" do CA CMDB com o atributo de fornecedor "mdr_memory" para todos os fornecedores chamados "myMdr" ou iniciando com "MDR". Além disso, o "physical_memory" é equacionado com o "phys_mem" para todos os outros provedores.

```
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name_regexp=”MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=”.*">
```

Exemplo: ocultamento de atributo

A instrução de metadados a seguir oculta o atributo "widget_cost" do fornecedor MDR para todos os fornecedores chamados "myMdr".

<macro name=cmdbMetadata hide_provider_attr="YES”
provider_attr="widget_cost" provider_name="myMdr">

Exemplo: Definindo um rótulo de atributo

A instrução de metadados a seguir define um nome de atributo “ext_mem_capacity” usando o rótulo “External Memory Capacity” na categoria de atributos no Visualizador do CMDBf.

```
<macro name=cmdbMetadata  attr=”ext_mem_capacity” category="Attributes”
heading="External Memory Capacity” help="Total external memory">
```

Mais informações:

Como exibir valores de atributos do MDR com nomes de atributos do CA CMDB (na página 749)
Como ocultar atributos do provedor do MDR (na página 750)
Como definir os atributos do MDR sem equivalentes do CA CMDB (na página 751)
Definir metadados do provedor de dados do CMDBf (na página 751)

Como exibir valores de atributos do MDR com nomes de atributos do CA CMDB

Os metadados podem criar uma associação entre os atributos do fornecedor MDR e os atributos do CA CMDB para que eles sejam exibidos juntos para ver as diferenças e compartilhar os rótulos. Por padrão, os atributos MDR que não possuem um mapeamento são exibidos como **Ausente do CMDB** na exibição.

Argumentos da macro do cmdbMetadata para equacionar um atributo do CA CMDB incluem:

- attr – nome de atributo do CA CMDB
- provider_attr – nome de atributo do fornecedor de MDR
- provider_name – Nome do fornecedor de MDR
- provider_name_regexp – expressão regular do nome do fornecedor de MDR

provider_name ou provider_name_regexp são obrigatórios.

Exemplo: associar os atributos do MDR aos nomes de atributo do CA CMDB

As três instruções de metadados a seguir para essas ações respectivas:

- Equacione o atributo "phys_mem" do CA CMDB com o atributo do fornecedor "mdr_memory" para todos os fornecedores chamados "myMdr".
- Equacione o atributo "phys_mem" do CA CMDB com o atributo do fornecedor "mdr_memory" para todos os nomes de fornecedores iniciados com "MDR".
- Equacione o "physical_memory" com o "phys_mem" para todos os outros provedores.

```
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem"  provider_attr="physical_memory"
provider_name_regexp=".*">
```

Como ocultar atributos do provedor do MDR

Alguns dos atributos do fornecedor MDR não precisam ser exibidos na Federated View. Os metadados de um fornecedor de MDR podem estar ocultos para um fornecedor de MDR específico. Essa opção se aplica apenas aos atributos do fornecedor MDR e não se aplica aos atributos do CA CMDB.

Argumentos da macro do cmdbMetadata para ocultar um atributo do fornecedor incluem:

- hide_provider_attr – "YES" – oculta o atributo do fornecedor do MDR
- provider_attr – nome de atributo do fornecedor de MDR
- provider_name – Nome do fornecedor de MDR
- provider_name_regexp – expressão regular do nome do fornecedor de MDR

provider_name ou provider_name_regexp são obrigatórios.

Exemplo: ocultar um atributo MDR Apenas

A instrução de metadados a seguir pode ser usada para ocultar o atributo "widget_cost" do fornecedor MDR para todos os fornecedores chamados "myMdr".

```
<macro name=cmdbMetadata  hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

Como definir os atributos do MDR sem equivalentes do CA CMDB

É possível definir rótulos e texto de ajuda para os atributos do fornecedor do MDR que não correspondem a nenhum atributo do CA CMDB. Os atributos são rotulados como Ausente da família na Federated View.

Argumentos da macro do cmdbMetadata para definir um atributo do fornecedor MDR incluem:

- attr – nome de atributo do CA CMDB
- category - Nome da categoria em que o atributo é exibido
- heading - rótulo do cabeçalho para o atributo
- help - breve descrição do atributo

Exemplo: definir um atributo MDR Apenas

A instrução de metadados a seguir define um nome de atributo "ext_mem_capacity" usando o rótulo “External Memory Capacity” na categoria Atributos na Federated View.

```
<macro name=cmdbMetadata  attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

Definir metadados do provedor de dados do CMDBf

É possível controlar como os dados são exibidos na Federated View.

Para definir os metadados para o Visualizador do CMDBf

1. Com o Pintor de tela da web, abra o arquivo cmdb_metadata_federation_viewer_site_attr.htmpl.
2. Determine quais mudanças do metadado são necessárias.

   Observação: são fornecidos modelos de exemplo no arquivo.
3. Copie o modelo adequado e substitua os argumentos necessários de acordo com as instruções no arquivo.
4. Salve e publique as mudanças.

Capítulo 16: Gerenciando mudanças

Esta seção contém os seguintes tópicos:

Gerenciamento de mudanças no CA SDM (na página 753)
Componentes do gerenciamento de mudança (na página 754)
Exibir o calendário de mudanças (na página 756)
Responsabilidades do CAB (na página 756)
Responsabilidades do Gerenciador de mudanças (na página 758)
Definir tarefas para a função Gerenciador de mudanças (na página 760)
Categorias de mudança, status e níveis de risco (na página 761)
Exibir o Gerenciador de filas de requisições de mudança (na página 762)
Definir uma consulta armazenada de requisição de mudança (na página 762)
Configurar opções de Gerenciador de mudanças (na página 764)
Calendário de mudança (na página 764)
Como programar requisições de mudança (na página 779)
Como programar janelas de mudança (na página 784)
Análise de conflito e detecção de colisão (na página 788)
Visualização do CA Workflow (na página 789)
Change Management Process Definition para o CA Workflow (na página 791)
Console do CAB e geração de relatório (na página 814)
Avaliação de risco (na página 821)
Impact Explorer (na página 824)

Gerenciamento de mudanças no CA SDM

O gerenciamento de mudanças do CA SDM é um conjunto de recursos para Gerenciadores de mudanças, Coordenadores de mudanças e Membros do CAB (Comitê Executivo de Mudanças) coordenarem a revisão e aprovação de solicitações de mudança para componentes e serviços de IC. Por exemplo, os gerenciadores de mudanças podem revisar e aprovar todas as mudanças em componentes e serviços de IC para assegurar que nenhuma nova vulnerabilidade de segurança seja introduzida no ambiente de produção. O Gerenciador de mudanças lidera o CAB e é responsável pela aprovação final das solicitações de mudança.

O gerenciamento de mudanças inclui as seguintes funções:

- Acompanhar processos do ITIL relacionando mudanças de TI ao Gerenciamento de incidentes/problemas.

- Exibir informações de Gerenciamento de serviços para um IC, por exemplo, o número de mudanças registradas em um IC, datas de implementação de mudanças e mais.
- Detectar colisões quando várias requisições de mudança indicam mudanças ao mesmo IC simultaneamente.
- Criar e armazenar janelas de mudança no Calendário de mudanças.
- Criar uma requisição de mudança na exibição do calendário.
- Avaliar os riscos associados a uma mudança.

Observação: para obter informações mais detalhadas sobre o gerenciamento de mudanças, consulte as informações sobre Gerenciamento de mudanças na *Ajuda online*.

Componentes do gerenciamento de mudança

O gerenciamento de mudança inclui os seguintes componentes:

Calendário de mudança

Exibe uma exibição gráfica dos eventos de mudança (na página 764), incluindo todas as requisições de mudança programadas, que falharam e em andamento para os ICs e serviço em uma exibição de calendário (na página 779) configurável. O calendário também exibe datas de blackout, que são períodos de congelamento. Os usuários podem criar uma requisição de mudança a partir do menu de contexto em exibições de calendário diárias, semanais e mensais. O Gerenciador de mudanças, os analistas de nível 2 e os membros do CAB usam este recurso.

Agendador de mudanças

Exibe períodos de tempo programados (na página 785) durante os quais mudanças de IC podem ou não ocorrer no Calendário de mudanças. O Gerenciador de mudanças usa esse recurso para visualizar e criar programações de mudança e associações de IC durante o período de tempo.

Análise de conflito e detecção de colisão

Analise requisições de mudança para ajudar a identificar conflitos potenciais de implementação que podem aumentar o risco de falhas. O Gerenciador de mudanças usa este recurso.

Visualização do fluxo de trabalho

Exibe o processo de aprovação para requisições de mudança. O Gerenciador de mudanças usa este recurso.

Console do CAB e geração de relatório

Exibe um painel (na página 814) que facilita aprovações rápidas de requisições de mudança online que exigem aprovação do CAB.

No CA SDM, o Gerenciador de mudanças pode gerar um relatório com detalhes sobre as solicitações propostas para mudanças prontas para revisão do CAB e distribuir os relatórios eletronicamente para todos os membros do CAB.

Observação: os usuários com privilégios apropriados podem exibir relatórios predefinidos de conformidade, previsão, tendência e volume para gerenciamento de mudança no BusinessObjects InfoView com o CA Business Intelligence.

Avaliação de risco

Permite anexar avaliações de risco para cada requisição de mudança enviada. A opção de pesquisa de risco permite criar pesquisas para avaliar riscos e associá-los a categorias de mudança. A pesquisa de risco lista uma série de perguntas de escolha única ou múltipla.

Impact Explorer

Exiba relacionamentos IC-a-IC de ICs vinculados a uma requisição de mudança. O Impact Explorer é iniciado na página Detalhes de requisição de mudança para facilitar a análise de impacto (na página 824) sob demanda. O Gerenciador de mudanças usa este recurso.

Verificação de mudança

Verifica se as mudanças são executadas de forma precisa e se não há mudanças informais, para que o CMDB contenha a representação atual de todos os CIs gerenciados.

Exibir o calendário de mudanças

O CA SDM pode ativar diversos recursos de gerenciamento de mudança (em conformidade com os padrões ITIL e COBIT) para exibir ou criar requisições de mudança após selecionar um dia no *Calendário de mudanças*. Novas requisições de mudança são automaticamente programadas para o dia selecionado.

O Calendário de mudanças relata conflitos, inconsistências e riscos em potencial entre cronogramas de mudança, requisições de mudança e ICs. Você pode usar o calendário para entender mudanças iminentes e seu impacto potencial no ambiente de TI e muito mais.

Para exibir o calendário de mudanças

1. Clique na guia Calendário de mudanças.

   Os campos de filtro Calendário de mudanças aparecem.

2. Conclua os campos de busca para mostrar uma exibição de calendário mostrando o cronograma para as requisições de mudança de interesse.
3. Clique em Pesquisar.

   O calendário de requisição de mudança exibe informações que correspondem a seus critérios de pesquisa.

Responsabilidades do CAB

O CAB (Change Advisory Board - Comitê Executivo de Mudanças) coordena a revisão e a aprovação ou rejeição de requisições de mudança para componentes e serviços de IC. Os membros do CAB são responsáveis por:

- Revisar todas as mudanças importantes para sistemas de produção.
- Participar de todas as reuniões relevantes do CAB como exigido pelo Gerenciador de mudanças.
- Revisar todas as solicitações enviadas para mudanças para determinar seu impacto, os recursos necessários para implementá-las e todos os custos contínuos.
- Participar da programação e coordenação do calendário de mudanças.
- Ajudar a assegurar que todas as mudanças sejam adequadamente avaliadas e priorizadas.
- Participar de revisões depois que a instalação estiver concluída.

Mais informações:

Como funciona o processo do CAB (na página 757)
Atribuir membros ao grupo CAB (na página 757)

Como funciona o processo do CAB

O CAB é responsável por verificar todas as principais mudanças aos sistemas de produção Os membros do CAB são notificados de que uma requisição de mudança exige sua aprovação, é possível executar as seguintes ações:

1. Listar as requisições de mudança que o CAB deve analisar.
2. Abrir o Console do CAB e exibir as informações contidas na solicitação.
3. Exibir a justificativa comercial, o plano de implementação, os itens de configuração e a documentação de suporte a ser associada à solicitação e decidir aprová-la ou rejeitá-la.
4. Aprovar ou rejeitar a requisição de mudança. A próxima requisição de mudança na lista é exibida automaticamente.

   A pessoa que solicita essa mudança é notificada automaticamente de que o status do CAB é atualizado para a requisição de mudança.

Mais informações:

Responsabilidades do CAB (na página 756)

Atribuir membros ao grupo CAB

A página Atualização de membros permite atribuir membros a um grupo CAB.

Para atribuir membros ao grupo CAB

1. Na página Detalhes do grupo, selecione a guia Membros.
2. Clique em Atualizar membros.

   A página Pesquisa de contatos é exibida.

3. Insira os critérios de pesquisa para exibir os contatos desejados e clique em Pesquisar.

   A página Atualização de membros é exibida, listando os contatos correspondentes aos critérios de pesquisa.

4. Na lista da esquerda, selecione os contatos que você quer atribuir ao grupo. Para selecionar vários itens, mantenha pressionada a tecla CTRL enquanto clica com o botão esquerdo do mouse.

5. Após selecionar todos os contatos que você quer, clique no botão de seleção (>>).

   Os contatos selecionados passam para a lista Membros da direita.

6. Clique em OK.

   A página Detalhes do grupo é exibida, com os contatos selecionados listados na guia Membros.

Responsabilidades do Gerenciador de mudanças

O Gerenciador de mudanças é responsável por todo o processo de gerenciamento de mudança da empresa e pela aprovação final de requisições de mudança. Ele também gera relatórios de análise de métricas do gerenciamento de mudança e faz o seguinte:

- Revisa requisições de mudança e adiciona interessados apropriados e aprovadores, conforme necessário.
- Facilita a resolução de problemas, como detecção de colisões e conflitos de cronograma no calendário.
- Revisa a instalação e planos de contingência e alternativos para acessibilidade e estabilidade.
- Entende o risco de cada mudança e assegura que o nível de risco apropriado seja atribuído à mudança.
- Monitora mudanças para suas áreas respectivas para assegurar que elas satisfaçam às exigências do Gerenciamento de mudança de tecnologia.
- Representa suas áreas respectivas e comunica o impacto de mudanças de alto nível de risco em reuniões semanais do CAB.
- Facilita revisões depois da conclusão da instalação para instalações com problemas e mudanças com erros.
- Serve como ponto de escalonamento para solicitantes de mudança, interessados, aprovadores, implementadores e grupos de suporte.

Mais informações:

Como a função Gerenciador de mudanças funciona (na página 759)

Como a função Gerenciador de mudanças funciona

Gerenciadores de mudanças são responsáveis por monitorar requisições de mudança no ambiente operacional para garantir que os integrantes da equipe de operação estejam em conformidade com os processos e políticas de negócio. O Calendário de mudanças pode facilitar a resolução de ocorrências, como conflitos de requisições de mudança programando datas de blackout e períodos de congelamento durante os quais um IC ou conjunto de ICs pode ser alterado. Os Gerenciadores de mudanças também fazem o seguinte:

1. Supervisiona o Console do CAB, do qual aprovações online e rápidas de requisições de mudança e solicitações para mudanças são gerenciadas.
2. Organiza CABs com membros apropriados às requisições de mudança em consideração e conduz reuniões do CAB programadas regularmente para revisar requisições de mudança inseridas.
3. Cria relatórios com detalhes sobre as solicitações propostas para mudanças prontas para revisão do CAB e distribui eletronicamente os relatórios a todos os membros do CAB.
4. Executa uma revisão em tempo real de cada requisição de mudança e atualiza o registro com a decisão do CAB durante a reunião do CAB.
5. Usa o BusinessObjects InfoView para gerenciar relatórios de conformidade, previsão, tendência e volume e criam relatórios de sob demanda.
6. Representa sua respectiva área e comunica o impacto de mudanças de alto nível de risco em reuniões semanais do CAB.
7. Avalia o risco de cada mudança e assegura que o nível de risco apropriado seja atribuído à mudança.

Definir tarefas para a função Gerenciador de mudanças

Você pode definir tarefas para a função Gerenciador de mudanças

Para definir tarefas para a função Gerenciador de mudanças

1. Na guia Administração, selecione Segurança e gerenciamento de função, Gerenciamento de função, Lista de funções.

   A página Lista de funções aparece.

2. Selecione a função Gerenciador de mudanças.

   A página Change Manager Role Detail aparece.

3. Clique em Editar.

   A página Change Manager Update Role aparece.

4. Use as guias e campos a seguir para configurar tarefas e permissões de acesso para a função Gerenciador de mudanças:

   - Autorização
   - Acesso a funções
   - Interface Web
   - Gerenciamento de conhecimento
   - Visibilidade do documento KT
   - Guias
   - Formulários web de relatório
   - Recursos Ir
   - Acesso de leitura do inquilino
   - Acesso de gravação de inquilino

5. Clique em Salvar, Fechar janela.

   O registro da função Gerenciador de mudanças é atualizado.

Observação: para obter mais informações sobre as guias que aparecem na página Change Manager Role Detail, consulte as informações sobre Gerenciamento de funções na *Ajuda online*.

Categorias de mudança, status e níveis de risco

Você pode definir como requisições de mudança operam dentro de seu ambiente de serviço. Você pode editar valores padrão instalados com o CA SDM ou definir seus próprios valores.

Para gerenciar valores padrão de requisições de mudança

1. Selecione Service Desk, Requisições de mudança na guia Administração.
2. Expanda o nó Requisição de mudança e selecione *um* dos seguintes:
   - Categorias
   - Tipos de mudança
   - Códigos de fechamento
   - Status do conflito
   - Nível de risco
   - Pesquisa de risco
   - Status
   - Código de status da tarefa do fluxo de trabalho
   - Tipos de tarefa do fluxo de trabalho

   A página Lista do item selecionado aparece.
3. Selecione o item a ser editado.

   A página Atualizar detalhes aparece.
4. Use os controles disponíveis nas guias na parte inferior da página para definir como requisições de mudança operam dentro de seu ambiente.
5. Clique em Salvar, Fechar janela.

   O item atualizado aparece na lista.

Exibir o Gerenciador de filas de requisições de mudança

O Gerenciador de filas de requisições de mudança mostra as requisições de mudança, conflitos e tarefas programadas atribuídas a analistas de nível 2, gerenciadores de mudanças, coordenadores de mudanças ou membros do CAB. Os usuários podem exibir seus registros atribuídos e não atribuídos por prioridade.

Para exibir o Gerenciador de filas de requisições de mudança

1. Navegue até Requisições de mudança no Gerenciador de filas do CA SDM.
2. Expanda as pastas para mostrar pastas aninhadas do seguinte:
   - Itens fechados ou abertos, atribuídos ou não atribuídos
   - Conflitos resolvidos ou não resolvidos
   - Tarefas programadas que iniciam hoje ou na próxima semana.
3. Selecione a pasta dos itens que você quer consultar.

   A página Lista aparece.
4. (Opcional) Clique em Mostrar filtro e preencha um ou mais campos para especificar os critérios de pesquisa que restringem a lista aos comentários de interesse.
5. Clique em Pesquisar.

   A página Lista exibe resumos dos itens correspondentes aos critérios de pesquisa.
6. (Opcional) Clique no botão Editar na lista para exibir alguns campos adicionais que podem ser associados a um item.

Definir uma consulta armazenada de requisição de mudança

Definir as consultas armazenadas disponíveis a usuários no Gerenciador de filas da requisição de mudança é uma tarefa administrativa. Você pode modificar as consultas armazenadas predefinidas instaladas com o CA SDM ou definir suas próprias consultas armazenadas.

Para definir uma consulta armazenada de requisição de mudança

1. Selecione Service Desk, Dados de aplicativo, Consultas armazenadas na guia Administração.

   A Lista de consultas armazenadas aparece.

2. Selecione a consulta armazenada que quer editar.

   A página Detalhes da consulta armazenada aparece.

3. Clique em Editar.

   A página Atualizar consulta armazenada aparece.

4. Edite os valores dos campos conforme apropriado.

5. Clique em Salvar, Fechar janela.

   A consulta armazenada atualizada aparece na lista de consultas armazenadas.

Exemplo: definir uma consulta armazenada para listar requisições de mudança atribuídas a um CAB a que o usuário conectado pertence

Este exemplo demonstra como você pode criar uma consulta armazenada que liste somente requisições de mudança atribuídas a um CAB a que o usuário conectado pertence.

Para criar a consulta armazenada

1. Navegue até o Gerenciador de filas para a página Atualizar consulta armazenada.

2. Edite os valores dos campos como segue.

   a. Selecione Utilização do gerenciador de filas.

   b. Defina o tipo para Requisição de mudança.

   c. Insira a cláusula Where:

      ```
      cab.[group]group_list.member IN (@cnt.id) AND active = 1
      ```

3. Clique em Salvar, Fechar janela.

   A consulta armazenada aparece na lista de consultas armazenadas.

Mais informações:

Console do CAB e geração de relatório (na página 814)

Configurar opções de Gerenciador de mudanças

Você pode configurar opções para a função Gerenciador de mudanças

Para configurar opções de Gerenciador de mudanças

1. Selecione Gerenciador de opções na guia Administração.
2. Expanda o nó Ger. requisições de mudança.

   A página Lista de opções aparece.
3. Clique com o botão direito do mouse na opção que você quer e selecione Editar no menu de contexto.

   A página Atualizar opções aparece.
4. Edite as opções conforme apropriado.
5. Clique em Salvar, Fechar janela.

   A opção atualizada aparece na lista de opções.

Calendário de mudança

O *Calendário de mudanças* fornece uma visão gráfica de eventos de mudança com horas de início e fim da implementação definidas. Esta exibição de calendário da programação de mudanças fornece aos analistas e gerentes uma forma rápida de identificar quando eventos ocorrem e como afetam o ambiente, a organização e os recursos.

O calendário permite criar requisições de mudança de exibições diárias, semanais e mensais, além de exibir janelas de requisições de mudança globais para requisições de mudança programadas. Se existirem várias janelas de mudança em um mês, elas serão agrupadas em conjunto, como um grupo único de janela de contingência. Faça uma busca detalhada por uma exibição semanal ou posicione o mouse sobre as informações para ver os detalhes de cada janela.

Observação: você só pode exportar (na página 766) cronogramas de requisições de mudança, e não das Janelas de mudança.

Mais informações:

Adicionar informações de cronograma a uma requisição de mudança (na página 765)
Modelos de evento do iCalendar (na página 766)
Exportar cronogramas para iCalendar (na página 766)
Exibições de programação (na página 767)
Programando configuração de exibição (na página 769)

Adicionar informações de cronograma a uma requisição de mudança

Você pode adicionar informações de cronograma ao criar ou editar uma requisição de mudança.

Para adicionar informações de cronograma

1. Execute uma das seguintes ações:
   - Clique em Arquivo, Nova requisição de mudança.
   - Abra uma requisição de mudança e clique em Editar.
2. Preencha os seguintes campos do cronograma:

   Tipo

   Especifica o tipo de mudança ITIL como Padrão, Normal ou Emergência. Um valor padrão pode ser definido para uma categoria de mudança que o CA SDM usa para inicializar novas requisições de mudança da categoria.

   Data de início do cronograma

   Especifica a data inicial da requisição de mudança.

   Duração

   Especifica a duração da requisição de mudança no formato 00:00:00.

   O cronograma contém apenas as requisições de mudança com uma data inicial e duração de cronograma não vazia. O tipo é útil para agrupar requisições de mudança no cronograma, mas não afeta diretamente a programação.
3. Continue criando a requisição de mudança.
4. Clique em Salvar quando terminar.

   As informações do cronograma são adicionadas à requisição de mudança.

Modelos de evento do iCalendar

Os modelos de evento do iCalendar controlam as informações que são exportadas para o formato do iCalendar.

Os seguintes modelos predefinidos são instalados com o CA SDM:

- Alterar Cronograma
- KnowledgeScheduleCreation
- KnowledgeScheduleExpired
- KnowledgeScheduleReview
- KnowledgeScheduleStart

Observação: é possível editar os códigos predefinidos de modelo de evento do iCalendar, mas não excluí-los ou criar novos códigos.

Importante: A variável SchedExpMaximum em web.cfg controla o máximo de eventos permitidos para uma exportação. Aumentar o padrão (1000) pode causar instabilidade no sistema. Se tentar exportar mais que o valor especificado em SchedExpMaximum, será exibida uma mensagem recusando a solicitação de exportação.

Exportar cronogramas para iCalendar

O CA SDM permite exportar as requisições de mudança no formato iCalendar padrão. A troca de dados permite importar cronogramas de requisições de mudança para muitos aplicativos de calendário amplamente usados, incluindo o Microsoft Outlook e o Lotus Notes.

Observação: ao exportar cronogramas sobre alguns programas de calendário, selecionar a opção Abrir em vez de Salvar faz com que o arquivo seja importado incorretamente. Para evitar esta ocorrência nos programas de Gerenciamento de conhecimento e Requisição de mudança, selecione a opção Salvar em vez de Abrir. Após salvar o arquivo exportado, importe-o por meio da interface de programa de calendário. Você não pode exportar as Janelas de mudança (blackout e manutenção, mas somente as requisições de mudança.

Importante: Os dados exportados são baseados na exibição atual. Se você deseja exportar um intervalo personalizado de datas, como 32 dias, a exportação deve ser feita a partir da exibição de lista. Caso contrário, a exibição é truncada para um mês ou semana, e somente exporta essa quantidade.

Para mostrar o calendário de mudanças

1. Clique na guia Calendário de mudanças.

   Os campos de filtro Calendário de mudanças aparecem.

2. Complete os campos de pesquisa para mostra uma exibição de lista ou calendário que inclua as requisições de mudança relevantes.

3. Clique em Exportar.

   A página Schedule export é exibida.

   Importante: A variável SchedExpMaximum em web.cfg controla o máximo de eventos permitidos para uma exportação. Aumentar o padrão (1000) pode causar instabilidade no sistema. Se tentar exportar mais que o valor especificado em SchedExpMaximum, será exibida uma mensagem recusando a solicitação de exportação.

4. Insira o local em que deseja salvar um arquivo iCalendar.

   Um arquivo iCalendar contendo todos os eventos na exibição é salvo no local especificado.

Exibições de programação

O CA SDM fornece as seguintes exibições de programação:

Lista

Exibe uma página de lista classificada pelas datas de início e término da programação.

Mês

Exibe um calendário para todo o mês.

A exibição mostra as requisições de mudança em grupos, com cada entrada coletando uma ou mais requisições de mudança. Você pode exibir informações detalhadas sobre as requisições de mudança em um grupo ao passar com o mouse sobre o grupo ativado; pressionando Alt+Seta para a direita quando o foco estiver sobre o grupo ou clicando sobre o grupo para exibir seu conteúdo em uma exibição de n-dias.

Semana

Exibe uma semana inteira em uma única coluna, iniciando com o dia configurado como o primeiro dia da semana.

A exibição mostra mudanças individualmente e inclui informações detalhadas sobre cada requisição de mudança programada durante a semana.

Dia

Exibe as requisições de mudança de um único dia.

A exibição mostra mudanças individualmente e inclui informações detalhadas sobre cada requisição de mudança programada durante o dia.

***n* dias**

Exibe requisições de mudança do número de dias especificado em uma lista suspensa.

A exibição mostra mudanças individualmente e inclui informações detalhadas sobre cada requisição de mudança programada durante os dias selecionados.

Navegando pelas exibições de programação

É possível usar as teclas tab e de setas para navegar pelas exibições de programação. Estão disponíveis os seguintes atalhos de teclado:

Guia

Navega até uma data posterior. Use a partir da última célula na programação para navegar até o botão Pesquisar.

Shift+Tab

Navega até uma data anterior. Use a partir da primeira célula na programação para navegar até o botão Próximo mês.

Shift+Seta

Navega pelo calendário de data a data na direção da seta.

Seta para a direita

Exibe o menu de contexto da data ou evento em foco no momento. Se não houver nenhum menu contexto, navega até a próxima data superior (similar a Shift+Seta para a direita).

Alt+Seta para a direita

Exibe um pop-up de informações ao passar o mouse sobre a data ou evento em foco no momento. Se não houver nenhuma informação ao passar o mouse, navega até a próxima data superior (similar a Shift+Seta para a direita).

Seta para baixo

Navega até o próximo evento na célula atual. Se não houver nenhum evento na célula atual, ou se o foco já estiver no último evento, ele navega até a data na próxima célula abaixo (similar a Shift+Seta para baixo).

Seta para cima

Navega até o evento anterior na célula atual. Se o foco não estiver em um evento, ele navega até a data na próxima célula acima (similar a Shift+seta para cima).

Teclas de atalho da exibição de calendário

Cada exibição de programação oferece suporte ao acesso por teclas de atalho para seus botões. A seguir, são apresentadas as teclas de atalho suportadas:

Alt+0

Alterna para a exibição de lista.

Alt+1

Alterna para a exibição diária.

Alt+7

Alterna para a exibição semanal.

Alt+3

Alterna para a exibição mensal.

Alt+9

Alterna para a exibição de *n*-dias.

Alt+<

Move para o período de tempo anterior na exibição atual.

Alt+>

Move para o próximo período de tempo na exibição atual.

Programando configuração de exibição

Você configura as exibições de programação mensal e semanal especificando declarações pdm_macro na seção <head> dos formulários HTMPL que definem a programação. Recomendamos usar a exibição de origem do Pintor de tela da web para editar estes formulários.

Qualquer formulário que exiba uma programação deverá conter o seguinte:

- Uma macro schedConfig
- Pelo menos uma macro schedAttr
- Pelo menos uma macro schedGroup

As macros de configuração estão em um arquivo de origem separado referenciado por uma declaração pdm_include no arquivo de origem principal. Este arquivo permite configurar sua programação sem modificar o arquivo de origem principal.

Por exemplo, as macros de configuração para o formulário Calendário de mudanças, list_chgsched.htmpl, estão em um arquivo chamado list_chgsched_config.htmpl. Para a Programação do ciclo de vida do conhecimento, é possível modificar list_kdsched_config.htmpl usando as mesmas macros.

É possível localizar list_chgsched_config.htmpl e list_kdsched_config.htmpl no seguinte diretório:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

Macro schedConfig — Configurar programação

A macro schedConfig especifica que um formulário contém uma programação e fornece informações básicas de configuração. Os seguintes valores são argumentos válidos da macro:

autosearch=1|0

Especifica se o formulário de programação recarrega dados do servidor quando o usuário selecionar uma exibição fora do intervalo de data selecionado atualmente. Definir o valor para 1 (padrão) faz com que o formulário pesquise automaticamente quando o usuário seleciona uma exibição com um ou mais dias fora do intervalo de seleção de data do filtro de pesquisa. Definir o valor para 0 exige que o usuário pressione o botão Pesquisar para iniciar uma pesquisa.

defaultView=0|1|7|30|99

Especifica a exibição padrão para o filtro de pesquisa como 0 (lista), 1 (dia), 7 (semana), 30 (mês), ou 99 (n-dias).

A especificação para defaultView afeta apenas a exibição inicial do filtro de pesquisa. Após a exibição da programação, o CA SDM mantém automaticamente a seleção de exibição do filtro alinhada com a exibição atual.

Padrão: 30

firstday=0|1|2|3|4|5|6|7

Especifica o primeiro dia da semana na exibição mensal como um número entre 0 (domingo) e seis (sábado).

Padrão: 0

export=xxx|0

Especifica o nome de código do modelo usado para exportação no formato iCalendar. Definir o valor para 0 indica que o recurso e o botão de exportação estão desativados.

Padrão: ChangeSchedule.

legend=1|2|0

Especifica o local da legenda da programação mostrando o nome e a formatação dos grupos na programação. É possível definir o valor para 1 para posicionar a legenda acima da programação, ou 2 para posicioná-la abaixo da programação. Defina o valor para 0 para desativar a legenda.

Padrão: 2

maxGroups=0/*n*

Especifica o número máximo de grupos a serem exibidos em uma única célula da exibição mensal do calendário.

Se houver mais do que maxGroups programados para um único dia, o CA SDM exibe somente os primeiros maxGroups-1, e substitui o último com um hiperlink "..nn more changes" em que o usuário pode passar o mouse por cima ou clicar para ver a lista completa. Defina o valor para 0 para desativar este recurso e permitir um número ilimitado de eventos em uma célula do calendário.

Padrão: 4

nday=(n,n,...)

Especifica seleções para a lista suspensa para a exibição de n-dias.

A especificação é uma lista de contagens de dias que devem ser incluídos na lista suspensa, ou 0 para indicar que a lista suspensa de n-dias é suprimida da programação. O primeiro valor especificado é o padrão para a lista suspensa.

Padrão: (3,7,14,28)

round=(*hr,min*)|0

Especifica se as datas de início e término da programação são arredondadas ao coletar requisições de mudança ou documentos de conhecimento em grupos. Especifique round=0 para desativar o arredondamento.

Por padrão, as datas de início e término da programação agrupam objetos. Todas as datas no CA SDM incluem um horário e, sem arredondamento, objetos programados com uma diferença de até mesmo um minuto ficariam em grupos separados. O arredondamento determina o grupo após ajustar a data inicial para uma hora ou minuto mais cedo e a data de término para uma hora ou minuto mais tarde.

O valor de arredondamento especifica uma hora ou um minuto (mas não ambos). As horas são arredondadas para o múltiplo mais próximo do valor especificado, por exemplo:

round=(0,15) arredonda para o quarto de hora mais próximo

round=(0,30) arredonda para a meia hora mais próxima

round=1 arredonda para a hora mais próxima

round=12 arredonda para a metade do dia mais próxima (12:00 ou 00:00)

round=24 arredonda para o dia mais próximo

Padrão: (0,15)

timefmt=24hr|([am],[pm])

Especifica o formato das horas nas exibições de calendário da programação.

O valor padrão de 24h especifica que as horas são exibidas no formato 24 horas (0:01 - 23:59). O valor alternativo de (am,pm) especifica um sufixo para horários da manhã e tarde, ou ambos.

Observação: todos os argumentos schedConfig são opcionais.

Macro schedAttr — Especificar um atributo armazenado

A macro schedAttr especifica um atributo armazenado para cada item selecionado na lista. Atributos armazenados estão disponíveis ao passar o mouse sobre as informações na exibição mensal; para as informações detalhadas ou resumidas em outras exibições e na função JavaScript setSchedEvents(). Os seguintes valores são argumentos válidos da macro:

attr=xxxx

(Obrigatório) Especifica um atributo do objeto na programação, como uma requisição de mudança ou Documento de conhecimento. Os atributos com pontos são permitidos. O nome de atributo da palavra-chave CI*nn* pode ser usado no Calendário de mudanças para especificar que os primeiros *nn* ICs associados à requisição de mudança estão incluídos nas informações armazenadas.

Observação: este argumento é o único argumento obrigatório para a macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Armazena o atributo da tabela armazenada referenciada para um atributo SREL (ignorado para atributos não SREL). O nome do atributo especificado deve ser precedido por um ponto.

Padrão: .COMMON_NAME

label=

Exibe um rótulo para o atributo na exibição de n-dias.

Padrão: o Majic DISPLAY_NAME do atributo

ident=1|0

Especifica se o atributo é um identificador para o objeto (como um número de referência de uma requisição de mudança). Atributos de identificador são exibidos sem um rótulo à frente do nome do grupo que é exibido ao passar o mouse e na exibição de n-dias.

Padrão: 0

detail=1|0

Especifica se o atributo está incluído nas informações de detalhe mostradas em outras exibições que não mensais. Informações de detalhe são as informações mostradas quando a caixa de seleção Summary Only na exibição não está selecionada..

Padrão: 1

hoverInfo=1|0

Especifica se o atributo é incluído no pop-up de informação suspensa que é mostrado na exibição mensal quando o cursor do mouse é passado sobre um grupo, ou o usuário pressionar Alt+seta direita quando o foco estiver no grupo.

Padrão: 0

summary=1|0

Especifica se o atributo está incluído nas informações de detalhe mostradas em outras exibições que não mensais. Informações de detalhe são as informações mostradas quando a caixa de seleção Summary Only na exibição não está selecionada..

Padrão: 0

Observação: o CA SDM exibe atributos em informações resumidas, detalhadas ou que são exibidas ao passar o mouse na mesma ordem que suas macros schedAttr.

Macro schedGroup—Especificar um grupo de eventos

A macro schedGroup especifica o nome e o código de cores de um grupo de itens. A exibição mensal agrega todos os itens de um grupo em um único evento. Exibições que não a mensal exibem itens individuais no formato para o grupo a que pertencem. Os seguintes valores opcionais são argumentos válidos da macro:

grpname=xxx

(Obrigatório) Especifica o nome do grupo. A macro atribui automaticamente um número ao grupo e atribui o número a uma variável de JavaScript com um nome do formulário schedGroup_xxx, em que xxx é o nome do grupo. Esta variável pode ser usada na função JavaScript setSchedEvents() para criar um evento que pertença ao grupo.

Observação: este argumento é o único argumento obrigatório para a macro schedGroup.

label=xxx

Especifica um rótulo para o grupo. Se especificado, o rótulo é mostrado em todas as exibições.

legend=xxx|0

Exibe uma descrição do grupo para a legenda que é exibida na parte inferior da programação. Os grupos são mostrados na legenda se pelo menos um exemplo do grupo existir na exibição atual. Especificar 0 faz com que o grupo seja sempre excluído da legenda.

Padrão: 0

color=black|*color*

Especifica a cor do texto em itens deste grupo. É possível especificar a cor no formato CSS, seja uma cor web válida ou um valor hexadecimal precedido pelo símbolo #.

Exemplo: insira "#FF0000" ou "red" para vermelho.

Padrão: black

bgcolor=white|*color*

Especifica a cor do plano de fundo para itens deste grupo. É possível especificar bgcolor no formato CSS, seja uma cor web válida ou um valor hexadecimal precedido pelo símbolo #.

Exemplo: insira "#FF000" ou "red" para vermelho.

Padrão: white.

style=normal|bold|italic

Especifica o estilo do texto deste grupo no estilo normal, negrito ou itálico.

Padrão: normal.

Configurar janelas de blackout e de manutenção no Calendário de mudanças

Edite instruções PDM_MACRO em list_chgsched_config.htmpl para modificar cores, rótulos, legendas e ícones para janelas de mudança.

Observação: se você usar macros schedGroup para alterar a formatação de janelas no Calendário de mudanças, também deve atualizar *schedule.css* se desejar que a formatação seja consistente com o Agendador de mudanças.

Para configurar janelas de mudança

1. Abra o formulário *list_chgsched_config.htmpl* em um editor de texto ou WSP.

   Você pode localizar este arquivo no seguinte diretório:

   ```
   $NX_ROOT\bopcfg\www\htmpl\web\analyst\
   ```

2. Na macro schedGroup, modifique os seguintes instruções PDM_MACRO:

   Para janelas de manutenção:

   ```
   <PDM_MACRO NAME=schedGroup grpname=maintWindow
       bgcolor=lightgreen
       label="Manutenção"
       legend="Janela de manutenção"
       icon= "confirmation_12.png">
   ```

   Para janelas de blackout:

   ```
   <PDM_MACRO NAME=schedGroup grpname=blackoutWindow style=italic color=white
       bgcolor=black
       label="Blackout"
       legend="Janela de blackout"
       icon= "warning_12.png">
   ```

   bgcolor

   Especifica a cor do plano de fundo da janela.

   rótulo

   Especifica o rótulo da janela como Blackout ou Manutenção.

   legenda

   Especifica o texto da legenda como exibido no Calendário de mudanças.

   ícone

   Especifica um URL opcional para um gráfico da web de 12x12 pixels.

Este ícone aparece com uma requisição de mudança ou grupo no Calendário de mudanças se a requisição de mudança residir totalmente em uma janela de manutenção ou se sobrepuser a uma janela de blackout.

3. Salve o formulário.

   As janelas de mudança são configuradas.

A função JavaScript setSchedEvents()

A função JavaScript setSchedEvents() cria eventos na programação. Modifique esta função quando desejar exibir quaisquer objetos novos do grupo. Os objetos predefinidos do grupo são exibidos por padrão.

O CA SDM chama setSchedEvents() uma vez para cada objeto (requisição de mudança ou documento de conhecimento) selecionado pelo filtro de pesquisa da programação. A função cria eventos para o objeto chamando uma segunda função, schedEvent() e passando para a ID do grupo, data de início e data de término do evento.

A função pode criar qualquer número de eventos (incluindo zero) para um objeto. A função padrão setSchedEvents() para o Calendário de mudanças (list_chgsched.htmpl) cria um evento para cada requisição de mudança e agrupa requisições de mudança por tipo de mudança. Esta função é codificada da seguinte forma:

```
1.      function setSchedEvents( chg )
2.      {
3.      var grpnum;
4.      switch( chg["chgtype"] - 0 ) {
5.              case 100: grpnum = schedGroup_std;  break;
6.              case 300: grpnum = schedGroup_emer; break;
7.              default:  grpnum = schedGroup_norm; break;
8.      }
9.      chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.     }
```

O parâmetro case especifica a ID do tipo de mudança. Para listar as IDs de caso, consulte Criar um tipo de mudança.

A função possui um único argumento de um objeto JavaScript contendo os atributos especificados pelas macros schedAttr. O comando switch nas linhas 4-8 examina o atributo chgtype da requisição de mudança e atribui o número de grupo apropriado a partir de uma das variáveis schedGroup_xxxx definidas pelas macros schedGroup anteriores. Na linha 9, ele chama a função schedEvent() para criar um evento na programação, passando o número do grupo anteriormente atribuído e as datas de início e término da programação. As datas estão disponíveis no objeto do argumento porque foram especificadas nas macros schedAttr anteriores.

Como programar requisições de mudança

Você pode exibir o cronograma de todos os itens de configuração associados a uma requisição de mudança. Considere as informações sobre programação ao criar, editar ou exibir uma requisição de mudança ou ao atualizar o Calendário de mudanças. Exibir o cronograma pode ajudar a evitar colisões de cronograma.

Para exibir e atualizar um cronograma, faça o seguinte:

1. Crie ou abra uma requisição de mudança.
2. Associe ICs à requisição de mudança.

   Observação: se você não associar um IC à requisição de mudança, um erro aparecerá ao clicar no botão Agendador.

3. Clique em Exibir agendador.

   O Agendador de mudanças aparece e mostra as seguintes exibições:

   Diário

   (Padrão) Exibe o período de tempo da requisição de mudança para a data e hora selecionada. Se nenhuma data estiver associada à requisição de mudança, o dia atual é exibido como padrão.

   Semanal

   Exibe o período de tempo da requisição de mudança na semana atual e inclui a data inicial de implementação, que pode ser configurada para a data inicial do Calendário de mudanças.

   Observação: a duração do cronograma determina o comprimento de sombreamento no cronograma. Por exemplo, se você criar uma requisição de mudança com duração de duas horas, o sombreado amarelo claro nas exibições do agendador aparece na duração das duas horas definidas.

4. (Opcional) Clique em um IC para exibir seus detalhes. Posicione o cursor do mouse sobre o nome do IC para exibir o nome completo.
5. (Opcional) Modifique a data de início de implementação ou a duração.
   a. Clique em Exibir cronograma para exibir o cronograma atualizado.
   b. Clique em Atualizar cronograma para atualizar o cronograma.

   Observação: você pode modificar o cronograma somente em modo de edição.

6. Salve a requisição de mudança.
7. Atualize o Calendário de mudanças para exibir janelas de mudança associadas a IC e globais.

Exemplo de uso do agendador de mudanças

O exemplo a seguir demonstra como usar o agendador de mudanças ao criar uma requisição de mudança.

1. Na guia Service Desk, selecione Arquivo, Nova requisição de mudança.

   A página Criar requisição de mudança aparece.

2. Selecione Atualizar ICs na guia Itens de config. Guia Itens.

   A página Pesquisa de item de configuração aparece.

3. Criar ou pesquisar ICs.
4. Usando a página Atualização de itens de configuração afetados, adicione ICs à requisição de mudança.
5. Clique em OK.

   A página Criar requisição de mudança é atualizada.

6. Clique no botão Agendador.

   A página Cronograma para a requisição de mudança aparece.

7. Selecione uma exibição e siga *qualquer* um dos seguintes procedimentos:
   - Clique nas células da tabela para modificar a data de início do cronograma.
   - Clique na data de início do cronograma para usar o Calendário.
8. Modifique a duração e clique em Exibir cronograma.

   O cronograma exibe suas mudanças.

9. Clique em Atualizar cronograma.

   O cronograma é atualizado com suas mudanças.

10. Salve a requisição de mudança.

Definir o número máximo de ICs

Você pode definir o número máximo de ICs exibidos no agendador de mudanças.

Para definir o número máximo de ICs

1. Abra *NX.env*.

   Você pode localizar este arquivo no seguinte diretório:

   ```
   $NX_ROOT\
   ```

2. Modifique o valor de *@NX_CHANGE_SCHEDULER_MAX_CI_CNT* para o número máximo que você quer.

   Observação: por padrão, a variável é definida como 100. Se um número máximo de ICs acima de 100 for definido, somente os primeiros 100 serão exibidos e você receberá um aviso.

3. Salve *NX.env* e ative o ciclo do CA SDM.

   O número máximo de ICs é definido.

Exemplo: definir o número máximo de ICs como 25

Na configuração a seguir, somente os primeiro 25 ICs aparecerão no agendador de mudanças.

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```

Modificar a cor do plano de fundo da duração da requisição de mudança

Você pode alterar a cor do plano de fundo da duração da requisição de mudança. Modifique as linhas a seguir em *schedule.css* para alterar o realce da barra de duração da requisição de mudança verde.

Para alterar a cor do plano de fundo

1. Abra *schedule.css*.

   Você pode localizar este arquivo no seguinte diretório:

   ```
   $NX_ROOT\bopcfg\www\wwwroot\css
   ```

   Importante: O $NX_ROOT\sdk também contém um arquivo chamado schedule.css com comentários úteis sobre controles css.

2. Modifique as linhas a seguir com o código de cor que você quer:

   ```
   td.noBorderBackColor{border-left:none;border-right:none;background-color:#F6E
   3CE;}
   td.withBorderBackColor{border-right:none;border-left:1px
   solid;background-color:#F6E3CE;}
   ```

3. Salve *schedule.css*.

No exemplo seguinte, a cor do plano de fundo da duração de mudança é #FF0000.

Exemplo: modificar a cor do plano de fundo da duração de mudança para #FF0000

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#FF0000;
}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#FF0000;}
```

Modificar cores na janela de mudança no Agendador de mudanças

Você pode alterar as cores que indicam janelas de mudança modificando linhas em *schedule.css.*

Observação: se você modificar *schedule.css* para alterar a formatação de janelas no Calendário de mudanças, também deve modificar as macros schedGroup usadas pelo Calendário de mudanças se desejar que sua formatação seja consistente com o Agendador.

Para alterar a cor do plano de fundo

1. Abra *schedule.css* em um editor de texto.

   Você pode localizar este arquivo no seguinte diretório:

   ```
   $NX_ROOT\bopcfg\www\wwwroot\css
   ```

2. Modifique as linhas a seguir com o código de cor que você quer:

   ```
   .schedConflict { background-color: #ff0000; font-size: 4px }
   .schedBusy { background-color: #0176ff; font-size: 4px}
   .schedCurrent { background-color: #008000; font-size: 4px; }
   .schedMW { background-color: #40ff40; font-size: 4px; }
   .schedBW { background-color: black; font-size: 4px; }
   .schedNone {font-size: 4px; }
   .schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;
   margin-top: 4px; margin-bottom: 4px; }
   ```

3. Salve *schedule.css*.

   A cor do plano de fundo é modificada.

Mais informações:

Macro schedConfig — Configurar programação (na página 770)

Como programar janelas de mudança

Você pode programar janelas de mudança e exibi-las no Calendário de mudanças. *A Janela de manutenção* estabelece períodos de tempo em que as mudanças no IC ocorrerão, e as *janelas de blackout* estabelecem os períodos de tempo em que as mudanças do CI *não* devem ocorrer. As janelas de mudança ajudam a programar mudanças para minimizar seu efeito em processos de negócio cruciais. O CA SDM pode implementar janelas de mudança no nível de sistema ou global.

Para programar janelas de mudança, faça o seguinte:

1. Visualize o Calendário de mudanças para ver onde você deseja alterar janelas.
2. Crie as janelas adequadas para a sua organização.

   Janela de manutenção

   Indica um período programado durante o qual um IC ou um conjunto de ICs pode ser alterado. Como as mudanças podem envolver tempo de inatividade, essas janelas podem ser usadas para minimizar perturbações a processos críticos para a organização. Em geral, mudanças programadas devem ocorrer dentro de uma janela de manutenção.

   Janela de blackout

   Indica um período programado durante o qual as mudanças de IC não devem ocorrer. Esta janela de blackout pode indicar um período de suporte reduzido (por exemplo, um feriado), um evento corporativo ou um momento crítico para a organização, como o término do ano fiscal. Em geral, as mudanças programadas só devem ocorrer fora das janelas de blackout.

   Janelas de mudanças globais

   Indica uma janela de blackout ou de manutenção que ocorrem para toda a organização. Por exemplo, você deseja criar uma janela de blackout global (na página 788) chamada Feriado que começa em Novembro e termina em Janeiro no fuso horário do leste dos Estados Unidos. Essa janela de blackout *não* permite mudanças não emergenciais entre essas datas. As janelas de mudanças globais não associam com os ICs específicos porque aplicam-se a todos os CIs.

3. (Opcional) Especifique os padrões de recorrência da janela de mudança.
4. Abra o Calendário de mudanças.

A legenda exibe ícones e cores para identificar janelas de mudança no cronograma.

5. Crie requisições de mudança associadas a ICs.
6. Atualize o Calendário de mudanças usando o Agendador de mudanças.

Observação: para obter mais informações sobre a criação de janelas de mudança, consulte a *Ajuda online*.

Exibir janelas de mudança

Você pode exibir janelas de mudança no Calendário de mudanças para ver quando ICs associados podem ou não ser alterados.

Para exibir janelas de mudança

1. Na guia Administração, clique em Service Desk, Requisições de mudança, Alterar janelas.

   A Lista de janelas de mudança aparece.

2. Selecione a janela de mudança que deseja exibir.

   A janela de mudança é exibida.

3. (Opcional) Clique em Editar.

   Você pode modificar a janela de mudança.

4. Salve ou feche a janela.

   A página Detalhes da janela é exibida.

Associar um IC com uma janela de manutenção

Para controlar quando um IC passa por manutenção, é possível associar esse IC a uma janela de manutenção.

Para associar um IC a uma janela de manutenção

1. Navegue até a página Detalhe da janela de mudança.
2. Clique na guia ICs associados.

   A lista ICs associados aparece.
3. Clique em Atualizar itens de configuração.

   A página Pesquisa de IC aparece.
4. Especifique as informações dos ICs obrigatórios.
5. Clique em Pesquisar.

   A página ICs disponíveis aparece.
6. Mova quaisquer IC obrigatórios na lista de ICs disponíveis para a lista de ICs associados.
7. Clique em OK.

   A página Detalhes da janela de mudança aparece.
8. Clique em Salvar.

   O IC é associado a uma janela de manutenção.

A janela de mudança, os ICs e as associações da janela selecionada são salvas.

Exibir ICs associados

Para determinar quais ICs podem ser afetados durante períodos de tempo específicos, é possível exibir os ICs associados com janelas de manutenção não globais.

Para exibir ICs associados a uma janela de manutenção

1. Navegue até a página Detalhe da janela de mudança.
2. Clique na guia ICs associados.

   Os ICs associados são exibidos.

Criar um exemplo de janela de blackout

O exemplo a seguir cria uma janela de blackout para indicar que a organização não programa requisições de mudança para um período de tempo específico. Você deseja que essa janela de blackout tenha duração de 48 horas e que se repita todas as sextas-feiras, às 18h00 de seu fuso horário.

Siga estas etapas:

1. Na guia Administração, clique em Service Desk, Requisições de mudança, Alterar janelas.

   A Lista de janelas de mudança aparece.

2. Clique em Criar novo.

   A página Criar janela de mudança aparece.

3. Preencha os campos apropriados da seguinte forma:

   a. Insira **Friday_Blackout** como o nome da janela.

   b. Selecione o tipo Blackout.

   c. Selecione o status Ativo.

   d. Selecione a próxima sexta-feira e 6:00 PM no Calendário como a data de início.

   e. Selecione o próximo domingo e 6:00 PM no Calendário como a data de término.

   f. Selecione seu fuso horário.

   g. (Opcional) Insira uma descrição para a janela de blackout.

   h. Na guia Modelo de repetição, selecione Semanal.

      - Defina a recorrência para a cada **1** semana.
      - Selecione a data para finalizar a recorrência.

4. Salve e feche a janela de blackout.

5. Atualize a lista de janelas de mudança.

6. Abra e atualize o Calendário de mudanças.

   A janela de blackout aparece no cronograma.

Criar uma janela de manutenção global

Criar uma janela de manutenção global para a sua organização. Por exemplo, você *não* deseja definir janelas de manutenção pelo servidor ou de IC e deseja realizar mudanças globais durante os finais de semana.

Siga estas etapas:

1. Navegue para a página lista de Janelas de mudança.
2. Clique em Criar novo.
3. A página Criar janela de mudança aparece.
4. Insira ou modifique os campos necessários para a janela de manutenção.
5. Defina o tipo para manutenção.
6. Verifique se a caixa de seleção Global está marcada.

   Observação: uma janela de manutenção global não pode ser associada a ICs.
7. Insira a Data inicial, a Data de término e o Fuso-horário.
8. Clique em Salvar.

   A janela de manutenção global é salva.

Análise de conflito e detecção de colisão

A análise de conflito detecta e mostra colisões que ocorrem quando duas ou mais mudanças no mesmo item de configuração são programadas para implementação no mesmo tempo. A equipe de gerenciamento de mudanças lida com colisões de cronograma da seguinte maneira:

- Usa o Calendário de mudanças para ver colisões de IC relacionadas a requisições de mudança e faz ajustes nelas para reduzir o impacto potencial.
- Pesquisa e detecta colisões em um log.

Observação: para obter mais informações sobre como lidar com colisões de cronograma, consulte a *Ajuda online*.

Visualização do CA Workflow

A visualização do CA Workflow permite monitorar o progresso de tarefas do fluxo de trabalho da requisição de mudança. O Visualizador de processos exibe graficamente cada etapa do processo do CA Workflow, incluindo etapas concluídas ou não e o local atual de uma progressão de fluxo de trabalho.

O Visualizador de processos exibe o status e o caminho de um processo do CA Workflow associado a uma categoria de mudança/ocorrência ou a uma área de solicitação/incidente/problema.

Como visualizar o fluxo de trabalho

Visualize o fluxo de trabalho como segue:

1. Associe um processo do CA Workflow a uma categoria de mudança.
2. Crie uma requisição de mudança usando essa categoria de mudança.
3. Na guia Tarefas do fluxo de trabalho, clique no botão Exibir processo para iniciar o Visualizador de processos.

Observação: para obter mais informações sobre como associar processos do CA Workflow a categorias ou áreas, consulte a *Ajuda online*.

Exemplo de uso do Visualizador de processos

Este exemplo demonstra como usar o Visualizador de processos em seu sistema com uma categoria de mudança padrão após instalar e ativar as opções do CA Workflow.

1. Na guia Administração, navegue para Service Desk, Requisições de mudança, Categorias.

   A página Lista de categorias de mudança aparece.

2. Selecione Add.IT.Other na coluna Símbolo.

   A página Detalhes da categoria de mudança de Add.IT.Other aparece.

3. Clique em Editar.

   A página Atualizar categoria de mudança Add.IT.Other aparece.

4. Clique na guia Fluxo de trabalho.

   Clique na caixa de seleção CA Workflow.

   A Lista de definições de fluxo de trabalho aparece.

5. Selecione Pedir PC - Service Desk Release 12.7.

   O nome de processo preenche o campo Nome da definição do CA Workflow.

6. Clique em Salvar.

   A página Detalhes da categoria de requisição de mudança é atualizada.

7. Feche a janela.

8. Crie e salve uma requisição de mudança usando a categoria Add.IT.Other.

   A guia Tarefas do fluxo de trabalho exibe o processo Pedir PC - Service Desk Release 12.7 e a lista de itens de trabalho.

9. Clique no botão Exibir processo na guia Tarefas do fluxo de trabalho.

   O Visualizador de processos aparece.

   Observação: você pode atualizar o Visualizador de processos para exibir o progresso atualizado das tarefas do fluxo de trabalho.

Change Management Process Definition para o CA Workflow

A Change Management Process Definition gerencia as requisições de mudança Padrão, Normal ou Emergência. Como parte do CA Workflow, a Change Management Process Definition gerencia todas as tarefas de requisições de mudança desde a solicitação inicial de mudança até a Revisão pós-implementação. À medida que cada tarefa é concluída, a Change Management Process Definition atualiza o status da requisição de mudança e o log de atividades. A Change Management Process Definition também envia por email ao contato ou grupo tarefas que exigem conclusão.

A Change Management Process Definition inclui as seguintes funcionalidades:

- Analisa o tipo de requisição de mudança e nível de risco associado para determinar o nível necessário de aprovações para implementação de mudança.
- Fornece uma base de exemplo como uma base para gerenciamento de mudanças.
- Alinha-se aos padrões ITIL v3 quanto à avaliação de risco, análise de impacto e conflito, e aprovações pelo Gerenciador de mudanças e pelo CAB.
- Incorpora a seguinte funcionalidade de Gerenciamento de mudanças do CA SDM:
    - Risk Assessment Survey
    - Caso de negócio
    - Análise de conflito
    - Análise do impacto
    - Códigos de fechamento
    - Códigos de status
    - Tipo de mudança
    - CAB e sinalizadores de aprovação do CAB

Mais informações:

CA Workflow (na página 293)

Componentes da Change Management Process Definition

A Change Management Process Definition tem os seguintes componentes:

- **Change Management Process Definition**—A definição de processo que gerencia todo o processo de requisição de mudança. Todas as atividades e subatividades seguem as boas práticas do CA Workflow atuais para tratamento de exceção. O nome do arquivo da definição de processo é *r12_Change_Mgmt_[en_language].xml*. Por exemplo, o nome da definição de processo em inglês é r12_Change_Mgmt_en_US.xml.

  Observação: para obter informações sobre boas práticas do CA Workflow, consulte https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/7956/7956_tecdoc.html.

- **Get Group Mem and Notify Process Definition**—Um bloco de construção que gerencia notificações de email para grupos. A Get Group Mem and Notify Process Definition aceita a UUID de grupo como entrada. Dependendo do sinalizador de notificação, a dGet Group Mem and Notify Process Definition pode enviar email a cada membro do grupo ou apenas ao gerente do grupo. O nome do arquivo da definição de processo é *r12_Get_Group_Mem_Notify_[en_language].xml.* Por exemplo, o nome do arquivo de definição de processo em inglês é r12_Change_Mgmt_en_US.xml.

- **Get Group Mem and Notify Actor**—Um representante que chama a Get Group Mem and Notify process definition. O nome de arquivo do representante é *r12_Get_Group_Mem_Notify_Actor_[en_language].xml*. Por exemplo, o nome, em inglês, do arquivo do representante é r12_Get_Group_Mem_Notify_Actor_en_US.xml

- **Date and Time Convert**—Um representante que aceita a data e hora como entradas e fornece uma sequência de caracteres de data e hora legível para campos de Data de início programada e Data de término programada em formulários de aprovação. O representante de Date and Time Convert é um representante de JavaScript do CA Workflow. O nome de arquivo do representante é *r12_Date_Time_Convert_Actor_[en_language].xml*. Por exemplo, o nome do arquivo do representante em inglês é r12_Date_Time_Convert_Actor_en_US.xml.

Como configurar a Change Management Process Definition

Para configurar a Change Management Process Definition, faça o seguinte:

1. Use o CA Workflow para verificar a documentação (na página 793) sobre nós de atividade, subatividades e notificações.
2. Crie os grupos CAB e de implementação (na página 795) que são responsáveis por gerenciar o processo de mudança.
3. Crie contatos (na página 796) e os atribua aos grupos CAB ou de implementação.
4. Configure notificações por email (na página 794) para a Change Management Process Definition.
5. Se não estiver usando a porta padrão do servidor Tomcat 8090, configure o servidor Tomcat (na página 797) para as comunicações apropriadas entre o CA Workflow e o CA SDM.
6. Configure uma ou mais categorias de mudança (na página 797) para usar a Change Management Process Definition.
7. Instale a opção Category Defaults (na página 798) no Gerenciador de opções.

Exibir documentação sobre nós de atividade e atributos

Como todos os nós de atividade e atributos dentro da Change Management Process Definition são documentados, é possível usar CA Workflow para exibir informações sobre nós de atividade e atributos. Se necessário, você pode alterar o fluxo da definição de processo para atender às necessidades de sua empresa.

Observação: para obter informações sobre visualização de nós de atividade e atributos, consulte a documentação do CA Workflow.

Para exibir documentação sobre nós de atividade e atributos

1. Abra a definição de processo Change Mgmt – Service Desk r12.1 no aplicativo CA Workflow.

   A Change Management Process Definition aparece no CA Workflow.

2. Clique duas vezes em um nó de atividade.

   O nó de atividade é aberto.

3. Na guia Propriedades, verifique o campo de Descrição para obter detalhes adicionais sobre o nó.
4. Saia das propriedades de nó de atividade.
5. (Opcional) Navegue até a guia Atributos na janela inferior da definição de processo.
6. Clique duas vezes ou passe o mouse sobre o atributo.

   A página Atributo é aberta com informações sobre o atributo.

Exibir subatividades

A Change Management Process Definition usa várias subatividades do CA Workflow para simplificar o fluxo de trabalho. Enquanto trabalha com a Change Management Process Definition, é possível verificar e personalizar as subatividades, caso necessário.

Para exibir subatividades

1. Abra a definição de processo Change Mgmt – Service Desk r12.1 no aplicativo CA Workflow.

   A Change Management Process Definition aparece no CA Workflow.

2. Clique com o botão esquerdo do mouse em qualquer nó com um símbolo de adição (+) e selecione Open Tab ou Open Inline.

   Os detalhes sobre a subatividade aparecem em uma nova guia ou próximo às atividades de definição de processo.

Como configurar notificações de email para os contatos de gerenciamento de mudanças

O sistema envia notificações de email sobre atribuições de tarefa de requisição de mudança e alterações de status. As notificações de email contêm links para a lista de trabalho ou requisição de mudança para verificação adicional. Como a Change Management Process Definition envia notificações de email, a configuração de email é obrigatória.

Para configurar notificações de email para contatos de Gerenciamento de mudanças, faça o seguinte:

1. Na guia Administração, selecione Gerenciador de opções, Opções de email.

   A página Lista de opções aparece.

2. Configure as opções de email conforme apropriadas para sua empresa.

Observação: para obter informações sobre configuração de email, consulte a *Ajuda online*.

Como criar grupos de processo de gerenciamento de mudanças

Ao criar grupos de processo de gerenciamento de mudanças que são responsáveis por aprovações e tarefas adicionais, considere o seguinte:

- é possível usar qualquer nome de grupo, contanto que os nomes do CA SDM e do CA EEM correspondam.
- O nome do grupo no CA SDM também deve corresponder ao nome da pasta do grupo no CA EEM.
- Cada grupo exige mais do que um membro.
- Os membros do grupo correspondem no CA SDM e no CA EEM. Por exemplo, se o grupo CAB do CA SDM tiver quatro membros, o grupo CAB do CA EEM tem os mesmos membros.

Observação: para obter informações sobre criação de grupos do CA SDM e do CA EEM, consulte a *Ajuda online* e a documentação do CA EEM.

Para criar grupos de gerenciamento de mudanças, faça o seguinte:

1. Na guia Administração, selecione Gerenciamento da segurança e funções, Grupos.

   A página Pesquisa de grupo aparece.

2. Clique em Criar novo.

   A página Criar grupo aparece.

3. Crie os seguintes grupos no CA SDM:

   - **Grupo CAB**—Um Grupo CAB que é associado à Categoria de mudança ou à requisição de mudança.
   - **Grupo de implementação**—Um grupo de implementação que é atribuído à Categoria de mudança ou à requisição de mudança.

4. Clique em Salvar.

   Aparece a página Detalhes do grupo.

5. Crie os mesmos grupos no CA EEM.

Mais informações:

Atribuir grupos CAB (na página 817)
Gerenciar grupos CAB (na página 815)

Como criar contatos do processo de gerenciamento de mudanças

Ao trabalhar com a Change Management Process Definition, você cria contatos que são responsáveis por aprovações e tarefas adicionais em todo o processo de mudança. Você também atribui os contatos aos grupos de Processo de gerenciamento de mudanças (na página 795).

Para criar contatos do processo de gerenciamento de mudanças, faça o seguinte:

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Contatos.

   A página Pesquisa de contato aparece.

2. Clique em Criar novo.

   A página Criar contato aparece.

3. Crie os seguintes contatos com endereços de email válidos e atribua-os aos grupos apropriados:

   - **Solicitante—**Um ou mais contatos que enviam a Solicitação para mudança.
   - **Gerenciador de mudanças**—O contato que é o gerente do grupo de implementação. O grupo de implementação só pode ter um gerenciador de mudanças.
   - **CAB Manager**—O contato que é o gerente do grupo CAB. O grupo CAB só pode ter um CAB Manager.

   A guia Contact Detail Groups lista as atribuições do grupo atual.

4. Na guia Membros da página de detalhes do Grupo de implementação, defina o sinalizador de Gerente para o Gerenciador de mudanças e o CAB Manager.

5. Clique em Salvar.

   A guia Membros exibe Gerente-Sim para os seguintes contatos:

   - Gerenciador de mudanças
   - CAB Manager

6. Crie os mesmos contatos no CA EEM e atribua-os aos grupos do CA EEM.

Observação: os nomes de contato podem usar qualquer nome de usuário ou logon de sistema válido. Para obter informações sobre criação de contatos do CA SDM e do CA EEM, consulte a *Ajuda online* e a documentação do CA EEM.

Especificar uma porta alternativa para o Servidor Tomcat do CA Workflow

Se o servidor Tomcat do CA Workflowestiver executando em uma porta diferente da porta padrão 8090, configure a porta para CA Workflow para se comunicar com o CA SDM.

Para especificar uma porta alternativa para o Servidor Tomcat do CA Workflow

1. Abra o aplicativo CA Workflow.

   A página do CA Workflow é exibida.

2. Clique na guia Representantes.

   A lista Actor Types/Actors é exibida.

3. Selecione JavaScript, USD_Initializer.

   A página Activity Options CA Workflow é exibida.

4. Clique duas vezes em Get Global Attributes.

   É exibida a página JavaScript Operation.

5. Altere o valor WFTomcatPort para a nova porta usada pelo Tomcat do CA Workflow.

6. Clique em OK.

   O Servidor Tomcat é configurado para o CA Workflow para se comunicar com o CA SDM.

Configurar a categoria de mudança

Quando você especifica a categoria de mudança para a Change Management Process Definition, cada nova requisição de mudança que usa a categoria executa automaticamente a Change Management Process Definition. Todos os valores de categoria de mudança pré-configurados preenchem automaticamente a requisição de mudança.

Para configurar a categoria de mudança

1. Na guia Administração, selecione Service Desk Manager, Requisições de mudança, Categorias.

   A Lista de categorias de mudança aparece.

2. Crie ou abra uma Categoria de mudança existente.

   A página Detalhes da categoria de mudança aparece.

3. Na guia Fluxo de trabalho, clique em Usar o CA Workflow.

4. Clique no link Definição do CA Workflow.

   A Lista de definições do CA Workflow aparece.

5. Clique em Change Mgmt - Service Desk r12.1.
6. Clique em OK.

   A página Detalhes da categoria de mudança aparece.

7. (Opcional) Atribua o CAB, Grupo e Pesquisa de risco.
8. Clique em Salvar.

   A próxima nova requisição de mudança que usar essa categoria automaticamente executará a Change Management Process Definition com os valores na categoria de mudança.

Observação: para obter informações sobre como criar ou editar Categorias de mudança, consulte a *Ajuda online*.

Instalar a opção Category_Defaults no Gerenciador de opções.

A opção Category_Defaults usa campos de categoria para preencher o CAB, Grupo e Pesquisa de risco na requisição de mudança. Por exemplo, o grupo CAB que você especifica para uma categoria aparece em todas as novas requisições de mudança que usam a categoria.

Para instalar a opção Category_Defaults no Gerenciador de opções

1. Na guia Administração, selecione Gerenciador de opções, Ger. requisições de mudança, Category_Defaults.

   A Lista de opções aparece.

2. Clique com o botão direito do mouse em Edit Category_Defaults.

   A página Category_Defaults Update Options é exibida.

3. Clique em Instalar.
4. Reinicie os serviços do CA SDM.

   As novas requisições de mudança automaticamente incluem valores da categoria.

Como funciona a Change Management Process Definition

Quando um solicitante salva uma requisição de mudança com uma categoria que usa a Change Management Process Definition, esta é chamada automaticamente.

As seguintes etapas descrevem como a Change Management Process Definition opera no CA SDM:

1. O solicitante abre e salva uma requisição de mudança que inclui as seguintes informações:

   Solicitador

      Identifica a pessoa que abriu a requisição de mudança.

   Categoria de mudança

      Identifica a categoria da requisição de mudança.

   Tipo

      Identifica o Tipo da requisição de mudança como alterações Padrão, Normais ou de Emergência. O Tipo também pode ser atualizado como parte do processo de Fluxo de trabalho.

   Resumo/Descrição

      Descreve a razão da requisição de mudança.

   Data de início programada

      Identifica a data de início.

   Duração

      Especifica a duração de tempo estimada para a mudança.

   ICs

      Identifica, pelo menos, um IC afetado.

   A Change Management Process Definition é executada. O solicitante recebe uma notificação por email para concluir a Risk Assessment Survey.

2. O solicitante verifica a requisição de mudança e conclui a Risk Assessment Survey (na página 806) que descreve como a requisição de mudança afeta servidores, aplicativos e usuários.

   A Change Management Process Definition analisa as respostas para determinar o risco e garantir que a requisição de mudança segue o caminho de processo apropriado. O solicitante recebe uma notificação por email para executar a análise de conflito e impacto.

3. Durante a análise de conflito e impacto (na página 807), o solicitante verifica se existem conflitos de programação e analisa o impacto da requisição de mudança nos ICs.

   O solicitante recebe uma notificação por email para executar a análise de mudança.

4. Durante a análise de mudança (na página 808),o solicitante identifica e envia o tipo de mudança, motivo da mudança, impacto de negócios e impacto total da mudança.

   O gerenciador de mudanças recebe uma notificação por email para aprovar a requisição de mudança. Se a requisição de mudança é um risco alto, o grupo CAB também recebe uma notificação.

5. O gerenciador de mudanças verifica a análise de mudança e insere comentários sobre a verificação. Ele aprova, rejeita ou marca a requisição de mudança como incompleta (na página 807).

   O sistema atualiza a página Detalhes da requisição de mudança da mesma forma e responde com uma das seguintes ações:

   - Se a requisição de mudança for aprovada e não for exigida nenhuma aprovação pelo CAB, o grupo de implementação recebe uma notificação. A requisição de mudança exibe o Status Aprovado.
   - Se a requisição de mudança for aprovada e forem exigidas aprovações adicionais pelo CAB, o gerente e membros do CAB recebem notificação para aprovação. A requisição de mudança exibe o Status Aprovação em andamento.
   - Se a requisição de mudança for rejeitada, ela exibe o Status Rejeitado.
   - Se a requisição de mudança for marcada como incompleta, ela exibe o Status Incompleto.

6. Para requisições de mudança aprovadas, um membro do grupo de implementação confirma o início da implementação (na página 811) e implementa a mudança.

   A requisição de mudança exibe o Status Implementação em progresso.

7. Quando o trabalho estiver concluído, o gerente de implementação conclui a PIR (na página 813)(Post Implementation Review - Revisão de pós-implementação) para descrever detalhes sobre o resultado da mudança.

   O CA Workflow fecha a requisição de mudança. A requisição de mudança exibe um Código de fechamento e o Status Implementado.

Mais informações:

Como configurar a Change Management Process Definition (na página 793)
Como implementar a pesquisa de risco (na página 821)
Exibir pesquisas de risco padrão (na página 822)

Como a CM Process Definition gerencia Aprovações de CO

O seguinte diagrama exibe como a Change Management Process Definition (na página 799) gerencia aprovações para uma nova requisição de mudança.

Ação do usuário
Definição de processo de gerenciamento de mudanças
Iniciar
O solicitante cria a requisição de mudança
Notificar o solicitante para que ele realize a avaliação de risco
O solicitante responde a pesquisa de avaliação de risco
Definir o status = RDM
Notificar o solicitante para que ele realize a análise de conflito e impacto
O solicitante realiza a análise de conflito e impacto
Notificar o solicitante para que ele realize a análise da mudança
O solicitante realiza a análise da mudança
Atualizar o tipo de mudança, o risco e o caso de negócios
Tipo de mudança?
2.Tipo de mudança = Padrão
3.Tipo de mudança = Emergência
4.Tipo de mudança = Risco normal, de médio a baixo
1.Tipo de mudança = Risco normal, de alto a extremo
Definir o sinaliza-dor de aprovação do CAB = Não
Definir o sinaliza-dor de aprovação do CAB = Não
Definir o sinalizador de aprovação do CAB = Sim
Enviar notificação do ECAB
Definir o status = Aplicativo em andamento
O gerenciador de mudanças aprova a requisição de mudança
Notificar o gerenciador de mudanças para que ele a aprove
1. Sim. Não requer a aprovação do CAB
2. Sim. Requer a aprovação do CAB
Recuperar o CAB e notificar sobre a aprovação
Notificar o grupo de imple-mentação para que ele conclua a requisição de mudança
Aprovada?
3. Rejeitar
Definir o status = Rejeitado Notificar o solicitante e o grupo de implementação para que executem novo trabalho
4. Incompleto
Definir o status = Incompleto Notificar o solicitante
Continuar

Como a CM Process Definition gerencia implementações de CO

O seguinte diagrama exibe como a Change Management Process Definition (na página 799) gerencia a implementação de requisição de mudança.

Implementação da requisição de mudança
Ação do usuário
Definição de processo de gerenciamento de mudanças
Entrada: Requisição de mudança aprovada
Continuar
Implementada?
Sim
Não
Status = Implementação concluída
Código de fechamento = Bem-sucedida
Notificar o solicitante
Notificar o grupo de implementação sobre a mudança desfeita
Status = Desfeita
Código de fechamento = Malsucedida
Notificar o grupo de Implementação para que ele verifique se a imple-mentação foi desfeita corretamente
Desfeita?
Malsucedida
Notificar o solicitante
Criar incidente
PIR em espera
Bem-sucedida
Notificar o solicitante
Notificar o grupo de implementação para que ele feche a PIR
PIR concluída pelo grupo de implementação
Fechar a requisição de mudança
Interromper

Concluir a Risk Assessment Survey

Ao criar uma requisição de mudança, o sistema notifica você para concluir a Risk Assessment Survey associada à categoria de mudança. Como solicitante, você identifica, avalia e quantifica os riscos de requisições de mudança que pertencem às categorias de mudança antes de modificar um sistema ou serviço.

Para concluir a Risk Assessment Survey

1. Abra a requisição de mudança clicando no link da notificação por email Risk Assessment Survey.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Requester Risk Assessment Survey e siga as instruções para concluir a pesquisa.

   A lista de trabalho do CA Workflow é exibida:

3. Na guia Tarefas, clique no link Executar.

   A página Perform Tasks aparece.

4. Faça uma observação das instruções e clique no link.

   A Pesquisa de risco aparece.

5. Preencha com cuidado as perguntas da pesquisa, de modo que o Change Management Process Workflow avalie de forma precisa o caminho de risco apropriado para a mudança

6. Clique em Enviar.

   A página Perform Task aparece.

7. Clique em Confirmar.

   A página de Detalhes da requisição de mudança mostra Status-RFC. O solicitante recebe uma notificação por email para executar a análise de conflito e impacto.

Mais informações:

Como acessar uma pesquisa de risco diretamente a partir de um URL (na página 823)

Realizar análise de conflito e impacto

Durante a análise de conflito e impacto, o solicitante verifica se existem conflitos de programação e analisa o impacto da requisição de mudança nos ICs.

Para executar a análise de conflito e impacto

1. Abra a requisição de mudança clicando no link da notificação por email.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Requester Impact and Conflict Analysis.

   Aparece a página Tarefas.

3. Na guia Tarefas, clique no link Executar.

   A página Perform Tasks aparece.

4. Faça uma observação das instruções da Análise de impacto e conflito e clique no link.

   A página Detalhes de requisição de mudança aparece.

5. Na guia Change Order Conflicts, clique em Análise de conflito para resolver todos os conflitos de programação e pendentes. Resolva todos os conflitos antes de implementar a mudança.

   A Conflicts List aparece.

6. Na guia Itens de config., clique em Análise do impacto para verificar os detalhes sobre os ICs.

   A Lista de itens de configuração aparece.

7. Em Config. de config., clique em Impact Explorer para analisar informações sobre cada IC.

   O Impact Explorer é aberto.

8. Clique em Visualizer para uma exibição gráfica dos relacionamentos de IC.

   Observação: o botão Visualizer só estará disponível quando o CA CMDB estiver instalado.

9. Retorne à página Perform task e clique em Confirmar.

   A guia Tarefas de fluxo de trabalho mostra um link para iniciar a análise de mudança. O solicitante recebe uma notificação por email para executar a análise de mudança.

Mais informações:

Impact Explorer (na página 824)
Iniciar o CMDB Visualizer a partir do Impact Explorer (na página 827)

Executar análise de mudança

Durante a análise de mudança, o solicitante identifica e registra as seguintes informações:

- Tipo de mudança
- Motivo para a mudança
- Impacto nos negócios
- Impacto geral da mudança

Para executar análise de mudança

1. Abra a requisição de mudança clicando no link da notificação por email.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Requester Change Analysis Form.

   Aparece a página Tarefas.

3. Na guia Tarefas, clique no link Executar.

   A página Change Analysis aparece.

4. Na guia Chg Analysis, responda às perguntas para confirmar a requisição de mudança e clique em Enviar. Por exemplo, resuma sua análise e explique o objetivo da requisição de mudança. Se necessário, especifique se a requisição de mudança é uma repetição ou retrabalho. Resuma o impacto nos negócios e impacto geral da mudança.

   Com base no tipo e risco da mudança, o sistema executa as seguintes ações:

   - Se o Tipo de mudança for Normal com risco alto a extremo, a página Detalhes da requisição de mudança mostra o seguinte:

     - Aprovação do CAB-Sim
     - Status-Aprovação em andamento

     O sistema notifica o Gerenciador de mudanças para aprovar a requisição de mudança. Por ocasião da aprovação pelo Gerenciador de mudanças, o grupo CAB é notificado para aprovação adicional.

- Se o Tipo de mudança for Normal com risco médio a baixo, a página Detalhes da requisição de mudança mostra o seguinte:
  - Aprovação do CAB-Não
  - Status-Aprovação em andamento

  O sistema notifica o Gerenciador de mudanças para aprovar a requisição de mudança.
- Se o Tipo de mudança for Padrão, o sistema notifica o grupo de implementação para implementar a mudança.
- Se o Tipo de mudança for de Emergência, a página de Detalhes da requisição de mudança mostra Aprovação CAB-Não.

  O sistema notifica o ECAB. Após o ECAB processar a requisição de mudança, a página de Detalhes da requisição de mudança mostra Status-Aprovação em andamento e o Gerenciador de mudanças recebe uma notificação para aprovar a requisição de mudança.

Aprovar, rejeitar ou marcar uma requisição de mudança como incompleta

O tipo de requisição de mudança e nível de risco norteiam o processo de aprovação para requisições de mudança que usam a Change Management Process Definition. Os seguintes valores de requisição de mudança determinam os aprovadores de requisição de mudança:

- Se o tipo for Normal e o risco for de médio a baixo, a requisição de mudança requer apenas a aprovação do gerenciador de mudanças.
- Se o tipo for Normal e o risco for de alto a extremo, a requisição de mudança exige aprovação do membro do CAB.
- Se o tipo for Padrão, não são necessárias aprovações. O sistema notifica o grupo de implementação para trabalhar na requisição de mudança.
- Se o tipo for de Emergência, o sistema notifica o grupo do ECAB. A requisição de mudança exibe o Status Aprovação em andamento. Quando a requisição de mudança está pronta para aprovação, o sistema notifica o gerenciador de mudanças.

Como aprovador, você verifica as informações de análise de mudança e determina se deve aprovar, rejeitar ou marcar a requisição de mudança como incompleta.

Para aprovar, rejeitar ou marcar uma requisição de mudança como incompleta

1. Abra a requisição de mudança clicando no link da notificação por email.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Change Manager Approval Form.

   Aparece a página Tarefas.

3. Na guia Tarefas, clique no link Executar.

   A página CAB or Change Manager Approval aparece.

4. Verifique a guia Chg Analysis para obter informações adicionais sobre a requisição de mudança.

5. Com base no nível de aprovação necessário, selecione uma das seguintes guias de aprovação e responda às questões de aprovação:

   Chg Mgr Approval

   Descreve a decisão do gerenciador de mudanças para a requisição de mudança.

   Aprovação do CAB

   Descreve a decisão do aprovador do CAB para a requisição de mudança.

6. Selecione um dos seguintes níveis de aprovação:

   Aprovar

   Aceita a requisição de mudança.

   Rejeitar

   Rejeita a requisição de mudança.

   Incompleto

   Marca a requisição de mudança como incompleta.

   Aparece a página Resultado. Com base no nível de aprovação, ocorrem as seguintes ações:

   - Se você aprovar a requisição de mudança e não for necessária nenhuma aprovação adicional do CAB, a página de Detalhes da requisição de mudança mostra Status-Aprovado, e o grupo de implementação recebe uma notificação para iniciar o trabalho.
   - Se você aprovar a requisição de mudança e for necessária a aprovação do CAB, a página de Detalhes da requisição de mudança mostra Status-Aprovação em andamento. O grupo CAB também recebe uma notificação.
   - Se você rejeitar a requisição de mudança, a página de Detalhes da requisição de mudança mostra Status-Rejeitado e o solicitante e o grupo de implementação recebem uma notificação.

- Se a requisição de mudança estiver incompleta, a página de Detalhes da requisição de mudança mostra Status-Incompleto e o solicitante recebe uma notificação.

Mais informações:

Como funciona o processo do CAB (na página 757)
Responsabilidades do CAB (na página 756)
Aprovações do CAB (na página 818)

Implementar uma requisição de mudança

Para uma requisição de mudança específica, um grupo de implementação conclui um ou mais itens de trabalho. Como membro do grupo de implementação, você relata informações sobre a mudança.

Para implementar uma requisição de mudança

1. Efetue logon no CA SDM como membro do grupo de implementação e abra a requisição de mudança.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Implement Change Order.

   A página Lista de tarefas aparece.

3. Na guia Tarefas, clique no link Executar.

   A página Perform Tasks aparece.

4. Siga as instruções para verificar a requisição de mudança e clique em Confirmar.

   A página de Detalhes da requisição de mudança mostra Status-Implementação em andamento.

5. Implementar a mudança. Por exemplo, se a requisição de mudança informou instalar o patch de AntiVirus no Exchange Server 1 e Exchange Server 2, conclua a requisição de mudança de acordo com as diretivas e normas da empresa.

6. Na guia Tarefas de fluxo de trabalho, clique no link Implement Complete Form.

   Aparece a página Tarefas.

7. Na guia Tarefas, clique no link Executar.

   A página Implementation Complete aparece.

8. Na guia Impl Complete, responda às questões para descrever como seu grupo implementou a requisição de mudança e clique em uma das seguintes opções:

   Concluído

   Especifica que todas as tarefas de requisição de mudança foram concluídas com sucesso. Define o Status da requisição de mudança como Implementation Complete e o Código de fechamento como Com êxito.

   Incompleto

   Especifica que um ou mais itens na requisição de mudança não puderam ser concluídos.

   O solicitante recebe um ou mais notificações sobre a conclusão ou retrocesso da requisição de mudança. O sistema também responde em uma das seguintes formas:

   - Se a requisição de mudança estiver concluída, a página de Detalhes da requisição de mudança mostra o seguinte:
     - Status-Implementation Complete
     - Código de fechamento-Com êxito.

     O sistema notifica o grupo de implementação para concluir a Revisão pós-implementação.

   - Se a requisição de mudança estiver incompleta, a página de Detalhes da requisição de mudança mostra o seguinte:
     - Status-Backed out
     - Código de fechamento-Sem êxito.

     O sistema também notifica o grupo de implementação para determinar se o retrocesso foi bem-sucedido.

     Quando o retrocesso é bem-sucedido, o sistema notifica o grupo de implementação para concluir a Revisão pós-implementação. Se o retrocesso é malsucedido, o sistema cria um incidente e notifica o grupo de implementação para concluir a Revisão pós-implementação.

Concluir a Revisão pós-implementação

Quando o trabalho é terminado, o grupo de implementação conclui a PIR (Post Implementation Review - Revisão pós-implementação) que descreve o resultado da mudança. Como membro do grupo de implementação, você tipicamente conclui a PIR de três a sete dias após a implementação da requisição de mudança. Entretanto, a Change Management Process Definition define um atraso padrão de dez segundos para a atribuição desta tarefa.

Para concluir a Revisão pós-implementação

1. Efetue logon no CA SDM como membro do grupo de implementação e abra a requisição de mudança.

   A página Detalhes de requisição de mudança aparece.

2. Na guia Tarefas de fluxo de trabalho, clique no link Revisão pós-implementação.

   A Lista de tarefas aparece.

3. Na guia Tarefas, clique no link Executar.

   A página PIR é exibida.

4. Na guia PIR, responda às questões para descrever a resolução e clique em Enviar.

   A página de Detalhes da requisição de mudança mostra Status-Fechado.

ActivityNode Actor not found: Update Object -Service Desk r12

Sintoma:

A janela de Comando do CA Workflow exibe o seguinte:

```
ActivityNode Actor not found: Update Object -Service Desk r12
```

Solução:

1. Efetue logon no aplicativo CA Workflow.
2. Clique na guia Actors.
3. Selecione a pasta Processes.

4. Selecione File/New Actor.
5. Selecione Update Object –Service Desk r12 na lista suspensa.
6. Clique em OK.

   Como parte da Change Management Process Definition, o sistema usa o novo representante.

A requisição de mudança não fecha

Sintoma:

Durante a última etapa no fluxo de trabalho, a requisição de mudança não fecha. A instância de processo do CA Workflow exibe o status Em execução e o CA Workflow informa um erro Actor Fault.

Solução:

Ao fechar a requisição de mudança, verifique se você definiu todos os campos obrigatórios, por exemplo, a Causa raiz.

Console do CAB e geração de relatório

O Console do CAB é um painel que facilita aprovações rápidas de requisições de mudança online que exigem aprovação do CAB. O Gerenciador de mudanças e outros membros do CAB usam o console para exibir detalhes sobre uma requisição de mudança (e suas tarefas do fluxo de trabalho e itens de configuração) e aprovam ou rejeitam a requisição de mudança. O Console do CAB permite a membros da equipe revisar, aprovar ou rejeitar uma requisição de mudança e avançar para a próxima requisição de mudança rapidamente. Para solicitações de requisição de mudança, o CAB pode lidar com a solicitação atendendo-as diretamente ou escalonando/encaminhando a solicitação a um grupo apropriado.

O Gerenciador de mudanças pode usar as opções de geração de relatório de detalhes e de resumo incorporadas do CA SDM para fazer o seguinte:

- Gerar relatórios de requisições de mudança aprovados e rejeitados
- Gerar relatórios de requisições de mudança esperando aprovação

Para imprimir ou exibir relatórios de resumo ou de detalhes, primeiro selecione os registros que você quer incluir no relatório. Você pode selecionar registros específicos para um relatório usando o recurso de pesquisa das páginas de lista.

Por exemplo, na lista de requisições de mudança, você pode inserir critérios de pesquisa para criar uma lista de requisições de mudança esperando aprovação do CAB, que pode ser usada para gerar um relatório.

Observação: para obter mais informações sobre como gerar relatórios de resumo e de detalhes no CA SDM, consulte as informações sobre a geração de relatório na *Ajuda online*.

Mais informações:

Gerenciar grupos CAB (na página 815)
Atribuir grupos CAB (na página 817)
Aprovações do CAB (na página 818)
Alterar propriedades do Console do CAB (na página 818)
Geração de relatório de gerenciamento de mudança (na página 820)

Gerenciar grupos CAB

Você pode criar e gerenciar grupos CAB com membros apropriados para as requisições de mudança em consideração. O CAB pode incluir membros da equipe de aplicativos, gerente de desenvolvimento, proprietário de componente, QA, suporte e todas as partes adicionais consideradas necessárias.

Observação: antes de implementar um grupo CAB, configure os contatos apropriados para sua estrutura comercial.

Para criar um grupo CAB

1. Na guia Administração, selecione Grupos.

   A página Pesquisa de grupo aparece.

2. Clique em Criar novo.

   A página Criar grupo aparece.

3. Preencha os campos conforme apropriado.
4. Clique em Salvar.

   O grupo CAB aparece na página Lista de grupos.

Para atribuir membros ao grupo CAB

1. Na página Detalhes do grupo, selecione a guia Membros.
2. Clique em Atualizar membros.

   A página Pesquisa de contatos é exibida.

3. Insira os critérios de pesquisa para exibir os contatos desejados e clique em Pesquisar.

   A página Atualização de membros é exibida, listando os contatos correspondentes aos critérios de pesquisa.

4. Na lista da esquerda, selecione os contatos que você quer atribuir ao grupo. Para selecionar vários itens, mantenha pressionada a tecla Ctrl enquanto clica com o botão esquerdo do mouse.
5. Após selecionar todos os contatos que você quer, clique no botão de seleção (>>).

   Os contatos selecionados passam para a lista Membros da direita.

6. Clique em OK.

   A página Detalhes do grupo é exibida, com os contatos selecionados listados na guia Membros.

Para adicionar o grupo CAB a uma categoria de mudança

Observação: assegure-se de que a opção Category_Defaults está instalada, de modo que o campo CAB em requisições de mudança defina um grupo CAB como padrão.

1. Na guia Administração, selecione CA SDM, Requisições de mudança, Categorias.

   A Lista de categorias de mudança aparece.

2. Selecione uma categoria na lista.

   A página Atualizar categoria de mudança aparece.

3. Selecione o grupo CAB apropriado do campo CAB.
4. Preencha os outros campos conforme apropriado.

5. Clique em Salvar.

   A página Detalhes da categoria de mudança exibe uma mensagem de salvamento bem-sucedido.

6. Clique em Fechar janela.

   O grupo CAB é associado à categoria de mudança e à requisição de mudança.

Mais informações:

Categorias requisições de mudança e ocorrência (na página 321)
Area_Defaults (na página 462)

Atribuir grupos CAB

Você pode atribuir um grupo CAB para revisar uma requisição de mudança antes de sua implementação.

Para atribuir um grupo CAB a uma requisição de mudança

1. Selecione a requisição de mudança desejada na lista de requisições de mudança.

   A página Detalhes de requisição de mudança aparece.

2. Clique em Editar.
3. Selecione CAB na área Detalhes.

   A página Lista de grupos aparece.

4. Selecione um grupo CAB.
5. Clique em Salvar, Fechar janela.

   O grupo CAB é atribuído à requisição de mudança.

Aprovações do CAB

O comitê executivo de mudanças (CAB) deve aprovar uma requisição de mudança antes da implementação da requisição de mudança se o campo Aprovação do CAB estiver definido como SIM. Durante o processo de aprovação, quando o gerenciador de mudanças clica em Aprovar ou Rejeitar, o status da requisição de mudança é alterado para Aprovado ou Rejeitado, respectivamente.

Observação: se quiser usar valores de status diferentes, você pode atualizar o código do botão Aprovar ou Rejeitar usando o Pintor de tela da web.

Mais informações:

Alterar propriedades do Console do CAB (na página 818)

Alterar propriedades do Console do CAB

Usando o Pintor de tela da web, você pode alterar as propriedades do Console do CAB exibidas em formulários web no Console do CAB. Por exemplo, é possível fazer o seguinte:

- Renomeie os botões Aprovar e Rejeitar. Estes botões são propriedades dos formulários web orderwf_approval_console.htmpl (tarefas do CA Workflow) e order_approval_console.htmpl (requisições de mudança).
- Personalize os valores de status dos botões Aprovar e Rejeitar alterando os valores de "REJ" ou "APR".
  - O botão 'Rejeitar tarefa' chama uma função approve_reject('REJ').
  - O botão ‘Aprovar tarefa' chama uma função approve_reject(‘APR’).

  Importante: Você somente pode associar uma transição ativa com um botão. Não desative uma transição de status predefinida que esteja associada a um botão, caso contrário, a transição de status predefinida não funcionará mais.

Para alterar propriedades do Console do CAB

1. Em Pintor de tela da web, abra o formulário Console do CAB que você quer alterar.

   O Pintor de tela da web abre e exibe o formulário.

2. Na guia Design, clique com o botão direito do mouse no controle que você quer alterar e selecione Propriedades.

   A página Propriedades - *controle* aparece.

3. Altere as propriedades que você quer inserindo novos valores para cada uma.

   As mudanças serão aplicadas assim que você clicar fora do campo ou fechar a página Propriedades.

   O Pintor de tela da web exibe um breve resumo do significado de uma propriedade em uma nota na parte inferior do formulário Propriedades quando você seleciona a propriedade.

Observação: para obter informações sobre o Pintor de tela da Web, consulte o *Guia de Implementação*.

Exemplo: personalizar o Console do CAB para alterar tarefas do fluxo de trabalho

Este exemplo mostra como personalizar o status de tarefa usando o Pintor de tela da web.

1. No Pintor de tela da web, abra o formulário web orderwf_approval_console.htmpl.

   O Pintor de tela da web abre e exibe o formulário.

2. Na guia Design, clique com o botão direito do mouse no botão Rejeitar tarefa e selecione Propriedades.

   A página Propriedades - Botão abre.

3. Localize a função approve_reject(‘REJ’).

   ‘REJ’ é o código de status para o status Rejeitar da tarefa.

4. Insira um novo valor para 'REJ'.

   As mudanças serão aplicadas assim que você clicar fora do campo ou fechar a página Propriedades.

   O Pintor de tela da web exibe um breve resumo do significado de uma propriedade em uma nota na parte inferior do formulário Propriedades quando você seleciona a propriedade.

Geração de relatório de gerenciamento de mudança

O Gerenciador de mudanças com privilégios apropriados pode usar o BusinessObjects InfoView para fazer o seguinte:

- Gerar relatórios de volume de mudança por sistema operacional, categoria de mudança, grupo, implementador, risco, status, data de implementação, ICs (Itens de Configuração) afetados e mudanças originadas de tickets de incidentes ou de problemas.
- Relatar mudanças com implementação bem-sucedida agrupadas por categoria da mudança, prioridade, impacto, % bem-sucedida vs. total para o período especificado e o grupo do solicitante da mudança.
- Relatar mudanças com implementação sem sucesso agrupadas por categoria da mudança, prioridade, impacto, % bem-sucedida vs. total para o período especificado e o grupo do solicitante da mudança.
- Gerar relatórios sobre o número total de requisições de mudança, agrupados por Coordenador de mudanças de categoria de mudança, Gerenciador de mudanças, nível de risco, prioridade e ICs afetados durante um período de tempo específico.

Você pode navegar para os relatórios predefinidos a seguir na seção esquerda da janela InfoView para exibir, programar, modificar ou executar o relatório, ou para exibir o histórico e as propriedades de um relatório.

Observação: para obter mais informações sobre como usar o BusinessObjects InfoView, consulte informações sobre o CA Business Intelligence na *Ajuda online*.

Avaliação de risco

As avaliações de risco permitem identificar, avaliar e quantificar os riscos de requisições de mudança pertencentes às categorias de mudança antes de modificar um sistema ou serviço em seu ambiente. Crie pesquisas de risco para avaliar riscos e associar as pesquisas a categorias de mudança. Quando um usuário cria uma requisição de mudança e especifica uma categoria de mudança, a pesquisa associada a essa categoria torna-se disponível para conclusão e envio.

A pesquisa de risco lista uma série de perguntas de escolha única ou múltipla. Cada resposta tem um valor ponderado. Ao criar uma requisição de mudança, o usuário seleciona as respostas apropriadas e envia a pesquisa. O nível de risco avaliado tem como base as médias ponderadas das respostas selecionadas pelo usuário.

Mais informações:

Exibir pesquisas de risco padrão (na página 822)
Implantar um exemplo de pesquisa de risco (na página 822)

Como implementar a pesquisa de risco

Implemente a pesquisa de risco como segue:

1. Estabeleça níveis de risco para sua organização.
2. Crie ou selecione uma pesquisa de risco na lista padrão.
3. Crie ou modifique perguntas e respostas de pesquisa de risco.
4. Modifique intervalos de risco para a pesquisa de risco.
5. Associe a pesquisa de risco a uma categoria de mudança.
6. Depois que você associar uma pesquisa de risco a uma categoria de mudança, o botão Risk Survey aparecerá para o solicitante quando ele salvar uma requisição de mudança usando a categoria de mudança especificada.
7. Exiba o risco avaliado com base nos resultados da pesquisa de risco.
8. (Opcional) Substitua o valor de risco avaliado no menu Atividades.

Observação: para obter informações detalhadas sobre como criar e modificar pesquisas de risco, consulte a *Ajuda online*.

Exibir pesquisas de risco padrão

O CA SDM fornece pesquisas de risco padrão que você pode associar a categorias de mudança.

Para exibir pesquisas de risco padrão

1. Navegue para Service Desk, Requisições de mudança, Pesquisa de risco.
2. Selecione Geral na coluna Nome da pesquisa de risco.

   A página Pesquisa de risco geral aparece.
3. Clique em Exibir pesquisa.

   A pesquisa de risco aparece, listando perguntas, respostas e valores de peso para cada resposta. Esta pesquisa se aplica a mudanças gerais dentro de sua organização.
4. Feche a pesquisa.
5. A página Pesquisa de risco geral aparece; feche-a.

Implantar um exemplo de pesquisa de risco

Este exemplo demonstra como implantar uma pesquisa de risco padrão em seu sistema usando uma categoria de mudança padrão.

1. Navegue para Service Desk, Requisições de mudança, Categorias.

   A Lista de categorias de mudança aparece.
2. Selecione Add.IT.Other na coluna Símbolo.

   A página de detalhes de Categoria Add.IT.Other aparece.
3. Clique em Editar.

   A página Atualizar categoria de mudança Add.IT.Other aparece.
4. Clique em Pesquisa de risco.

   A Pesquisa de modelo da pesquisa de risco aparece.
5. Procure a pesquisa de risco. Neste exemplo, pesquise Geral e selecione a pesquisa de risco para adicioná-la ao formulário de detalhes.

   O campo Pesquisa de risco é preenchido com Geral.
6. Salve e feche a janela.

Se um usuário criar uma requisição de mudança usando a categoria Add.IT.Other, o botão Pesquisa de risco aparecerá quando ele salvar a requisição de mudança.

Como acessar uma pesquisa de risco diretamente a partir de um URL

É possível fornecer um URL dinâmico para permitir que um usuário tenha acesso a uma Pesquisa de risco de requisição de mudança diretamente através de um URL de dentro de uma tarefa no CA Workflow. Você pode anexar este URL dinâmico com o parâmetro *KEEP.UsingURL=1* para indicar que a Pesquisa de risco está sendo acessada diretamente com um URL.

Crie um URL dinâmico dentro do CA Workflow da seguinte forma:

1. Abra sua Definição de processo do CA Workflow e adicione um nó de atividade para um usuário para concluir a Pesquisa de risco.
2. Dentro do nó de atividade, adicione um URL dinâmico usando a sintaxe apropriada. Verifique para anexar o parâmetro *KEEP.UsingURL=1*, tal como no seguinte exemplo:

```
http://<hostname>:CA Portal/CAisd/pdmweb.exe?CNT_ID=<ID of contact>+CRID=<ID of Change Order>+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

nome dohost

Especifica o nome de host do servidor do CA SDM.

port

Especifica a porta em que o CA SDM está instalado.

ID of Contact

Especifica a ID interna do contato concluindo a Pesquisa de risco.

ID of Change Order

Especifica a ID interna da Requisição de mudança associada à Pesquisa de risco.

O exemplo a seguir exibe um URL de amostra:

```
http://hostname:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A800
+CRID=400009+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

Importante: Se você não adicionar o parâmetro *KEEP.UsingURL=1* ao URL dinâmico, o usuário obtém um erro após enviar a pesquisa de risco, e o nível de risco não é calculado.

3. Salve a Definição do processo do CA Workflow.
4. Crie uma Categoria de mudança e associe uma Pesquisa de risco e a Definição do processo do CA Workflow para a Categoria de mudança.

   Salvar as mudanças
5. Abra uma Requisição de mudança com esta Categoria de mudança e salve-a para instanciar o Processo do CA Workflow.

6. Como parte do Processo do CA Workflow, um usuário é atribuído a uma tarefa para concluir a Pesquisa de risco. O usuário clica no URL, conforme descrito previamente.
7. O usuário efetua logon no CA SDM usando o URL e é levado diretamente no contexto da Pesquisa de risco para a Requisição de mudança.
8. O usuário envia a pesquisa e é exibida uma mensagem indicando o êxito ou falha.

   Se o envio for bem-sucedido, o nível de risco é calculado e atualizado na requisição de mudança.

Impact Explorer

O Impact Explorer é uma ferramenta avançada para gerenciar e controlar as mudanças dentro de uma organização. O Impact Explorer permite ao Gerenciador de mudanças explorar ICs vinculados a uma requisição de mudança, além de interagir diretamente com um IC vinculado ou seus ICs filho.

O Impact Explorer fornece estas vantagens:

- Exibe todos os ICs vinculados a uma requisição de mudança
- Exibe todos os relacionamentos filho e ponto-a-ponto para ICs vinculados
- Permite vincular qualquer IC relacionado à requisição de mudança
- Exibe uma lista de descendentes de ICs sucessivamente relacionados para qualquer IC vinculado
- Permite iniciar o CMDB Visualizer para um IC

Mais informações:

Iniciar o Impact Explorer (na página 825)
Explorar ICs vinculados (na página 825)
Exibir um IC no Impact Explorer (na página 826)
Adicionar um IC relacionado a uma requisição de mudança (na página 826)
Exibir a Lista de descendentes do IC (na página 827)
Iniciar o CMDB Visualizer a partir do Impact Explorer (na página 827)
Configuração do Impact Explorer (na página 828)

Iniciar o Impact Explorer

Você pode acessar o Impact Explorer da guia Itens de config. de qualquer requisição de mudança.

Para iniciar o Impact Explorer

1. Abra uma página Detalhes de requisição de mudança.
2. Selecione a guia Itens de Config. Guia Itens.
3. Clique em Impact Explorer.

   A página Impact Explorer aparece.

   Observação: se você fechar a página Detalhes de requisição de mudança, a página Impact Explorer também fechará.

Observação: se o Impact Explorer for iniciado de várias requisições de mudança, várias páginas Impact Explorer serão exibidas.

Explorar ICs vinculados

A árvore Impact Explorer contém um nó para cada IC vinculado a uma requisição de mudança. Um sinal de adição (+) indica que um IC tem ao menos um IC filho.

Observação: se mais de 100 ICs estiverem vinculados à requisição de mudança, somente os 100 primeiros serão exibidos.

Para exibir os relacionamentos de um IC vinculado, clique no sinal de adição (+) do IC. Os ICs relacionados são exibidos na árvore. Além dos nomes dos ICs relacionados, a árvore também exibe os tipos de relacionamento entre colchetes.

Observação: se a requisição de mudança tiver mais de 100 ICs vinculados, somente os 100 primeiros serão exibidos. Para exibir os próximos 100 ICs, clique em Mais...

Exibir um IC no Impact Explorer

A árvore Impact Explorer exibe um nó para cada IC vinculado a uma requisição de mudança. Um sinal de adição (+) indica que um IC tem ao menos um IC filho.

Para exibir um IC

1. Clique em um nó IC no painel esquerdo.

   A página Detalhes do item de configuração aparece na seção direita.

   Observação: você também pode exibir a página Detalhes do IC na seção direita clicando com o botão direito do mouse no IC e selecionando Exibir do menu de contexto.

2. Clique no nó da requisição de mudança no topo do painel esquerdo.

   A página Detalhes de requisição de mudança aparece.

Observação: se a requisição de mudança tiver mais de 100 ICs vinculados, somente os 100 primeiros serão exibidos. Para exibir os próximos 100 ICs, clique em Mais...

Adicionar um IC relacionado a uma requisição de mudança

Ao explorar relacionamentos de ICs, você pode optar por anexar um IC relacionado à requisição de mudança.

Para adicionar um IC relacionado a uma requisição de mudança

1. Clique em Config. Clique na guia Itens de config. para uma requisição de mudança.

   A página Lista de itens de configuração aparece.

2. Clique em Impact Explorer.

   A árvore do Impact Explorer exibe os ICs vinculados.

3. Clique em um sinal de adição (+) de um nó de IC vinculado.

   Os ICs relacionados ao nó aparecem.

4. Clique com o botão direito do mouse em um IC relacionado e selecione Adicionar a requisição de mudança no menu de contexto.

   O novo IC vinculado aparece na guia Itens de config. para a requisição de mudança.

Exibir a Lista de descendentes do IC

Para qualquer IC, você pode exibir linhas de ICs relacionados (denominados *descendentes*). Além das informações básicas sobre cada IC, a Lista de descendentes do IC exibe níveis de relacionamento, com o IC original como nível 1. Os ICs filho começam no nível 2, os filhos dele no 3 e assim por diante. Se um IC for encontrado mais de uma vez entre os relacionamentos rastreados, somente seu nível de relacionamento mais próximo será exibido.

Exemplo: vários caminhos de descendentes para um IC

Devido a vários relacionamentos, uma pesquisa de descendentes localiza o mesmo IC relacionado no nível 2 e no nível 4. O IC descendente é exibido somente no nível 2.

Para listar descendentes de um IC

1. Em uma página Detalhes de requisição de mudança, selecione a guia Itens de config. Guia Itens.
2. Clique em Impact Explorer para exibir os ICs vinculados.
3. Expanda um nó de IC se necessário.
4. Clique com o botão direito do mouse em um IC e selecione Listar descendentes.

   A Lista de descendentes do IC é exibida.

Iniciar o CMDB Visualizer a partir do Impact Explorer

O Impact Explorer permite iniciar o CMDB Visualizer de um IC vinculado ou relacionado.

Para iniciar o CMDB Visualizer do Impact Explorer

1. Em uma página Detalhes de requisição de mudança, clique em Impact Explorer.

   A página Impact Explorer aparece.
2. Clique com o botão direito do mouse em qualquer IC e selecione Launch Visualizer de seu menu de contexto.

   O CMDB Visualizer é iniciado com o IC como foco.

Configuração do Impact Explorer

Um administrador pode configurar o Impact Explorer como segue:

- Especificar o número de ICs filho um IC vinculado exibidos
- Especificar o número de níveis de relacionamento exibidos na Lista de descendentes do IC
- Suprimir a exibição de ICs filho

O número de ICs filho exibido é configurável, adicionando-se a configuração NX_IMPACT_EXPLORER_MAX_CHILD_NODES ao arquivo de configuração NX.env. O padrão é 100.

Exemplo: configurar a exibição de ICs filho

Usando a configuração a seguir, o Impact Explorer exibirá somente 10 filhos de um IC vinculado de cada vez:

@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10

A profundidade padrão da Lista de descendentes do IC é de nove níveis. É possível configurar a profundidade adicionando-se a configuração NX_IMPACT_EXPLORER_MAX_LEVELS ao arquivo de configuração NX.env.

Exemplo: configurar o número de níveis de descendentes

Quando você usa a configuração a seguir, a Lista de descendentes do IC exibe o IC original e somente seus ICs filho de relacionamento direto:

@NX_IMPACT_EXPLORER_MAX_LEVELS=2

Use a opção a seguir do Gerenciador de opções para suprimir a exibição de um determinado tipo de IC filho:

IMPACT_EXPLORER_EXCLUDE_HIER=boolean

Se a opção IMPACT_EXPLORER_EXCLUDE_HIER estiver instalada e definida como Sim, os ICs filhos relacionados na guia Relacionamentos do CMDB de página Detalhes de CI não serão exibidos na árvore Impact Explorer nem em Lista de descendentes do IC.

Observação: ICs filhos relacionados através do CA CMDB ainda são exibidos.

Capítulo 17: Gerenciando relatórios

Esta seção contém os seguintes tópicos:

Relatórios do CA Business Intelligence (na página 829)
Cenários de geração de relatórios (na página 830)
Componentes de relatórios (na página 831)
Diagrama do fluxo de dados da geração de relatório (na página 834)
Exibir relatórios no InfoView com base na web (na página 835)
Segurança e Autorização (na página 836)
Como apontar um servidor do CA Business Intelligence para um servidor do CA SDM (na página 842)
Como definir a segurança de partições de dados para a geração de relatórios (na página 845)
Banco de dados replicado para geração de relatórios offline (na página 847)
Relatórios de Role-Based (na página 847)
Relatórios com base na web (na página 857)
Principais indicadores de desempenho (na página 861)
Relatórios ad hoc (na página 873)
Exemplo de Relatórios ad hoc (na página 875)
Relatórios do painel (na página 880)
Gravar relatórios do CA Business Intelligence (na página 881)

Relatórios do CA Business Intelligence

O CA Business Intelligence é um componente com base na web que engloba a tecnologia de Business Objects, integrado com o CA SDM e uma variedade de fontes de dados comuns, como SQL Server, Oracle e Open Database Connectivity (ODBC).

O CA Business Intelligence usa BusinessObjects Enterprise como o sistema de geração de relatórios padrão. Relatórios predefinidos são fornecidos para o CA SDM, Gerenciamento de conhecimento e o Support Automation.

Com o sistema de geração de relatórios do CA Business Intelligence os usuários podem fazer o seguinte:

- Personalizar relatórios existentes
- Detalhar os dados de relatório do Business Objects para exibir os dados subjacentes aos gráficos e grupos resumidos

- Exportar instâncias de relatórios para diferentes formatos de saída
- Criar relatórios ad hoc
- Publicar novos relatórios e distribui-los a usuários autorizados
- Agendar relatórios para serem executados em horários específicos
- Use os relatórios do painel para monitorar operações diárias para todos os tipos de ticket do CA SDM.

Observação: o acesso à geração de relatório é restrito pela segurança de partição de dados do CA SDM.

Cenários de geração de relatórios

O CA Business Intelligence integrado ao BusinessObjects Enterprise oferece suporte aos seguintes cenários de geração de relatório:

- **Geração de relatório com base na função** — Na guia Relatórios do CA SDM, os usuários autorizados podem exibir relatórios definidos para sua função, depois clicar no botão InfoView para gerenciar seus relatórios pessoais no BusinessObjects InfoView. O CA SDM usa a interface do InfoView para coletar, organizar e apresentar informações em formatos de relatório. Em InfoView, os relatórios predefinidos são agrupados em pastas públicas.
- **Geração de relatório com base na web** — Relatórios com base na web são relatórios predefinidos no CA SDM, Gerenciamento de conhecimento, CMDB e Support Automation. São desenvolvidos com o Web Intelligence ou o Crystal Reports. Os relatórios são acessados no InfoView e podem ser usados como modelos para definir relatórios específicos do local.
- **Geração de relatório ad hoc** — Relatórios ad hoc são criados e administrados pelo InfoView com uma interface do Web Intelligence com base em plugin. Você pode armazenar e gerenciar relatórios em uma área de trabalho pessoal (My Folders). A geração de relatório ad hoc é destinada a usuários que queiram criar relatórios básicos facilmente sem a criação de consultas.
- **Geração de relatório de painel** — A geração de relatório de painel permite o monitoramento das operações diárias para todos os tipos de tickets do CA SDM (solicitação/incidente/problema, requisição de mudança ou ocorrência) no InfoView. Cada relatório contém dados analíticos sobre aqueles com os melhores desempenhos no trabalho com tickets ativos, para que você possa monitorar seu progresso. É possível trabalhar com relatórios individuais de painel predefinidos ou usar o painel corporativo para exibir todas as operações diárias do CA SDM em uma única exibição.

Componentes de relatórios

O BusinessObjects Enterprise e suas ferramentas associadas, juntamente com o BusinessObjects Crystal Reports XI são o backbone da arquitetura do CA BI.

Embora os relatórios do Crystal sejam entregues como o componente principal do CA Business Intelligence, ferramenta de manutenção e criação de relatório, o Crystal Reports XI, não é fornecido como parte do CA Business Intelligence. O Crystal Reports XI é um produto licenciado separadamente que pode ser adquirido a partir do BusinessObjects Enterprise e usado em conjunto com o CA Business Intelligence.

Observação: os relatórios predefinidos do Microsoft Access não são mais desenvolvidos ou fornecidos com o CA SDM.

É possível usar os seguintes componentes para administrar, monitorar e configurar o ambiente de criação de relatório do CA Business Intelligence:

- **Domsrvr/Driver ODBC/Banco de dados do CA SDM —** Os dados do relatório são armazenados em um banco de dados SQL Server ou Oracle do CA SDM. As aplicações de relatório BusinessObjects (Crystal Reports e Web Intelligence) acessam o banco de dados usando um driver ODBC que se conecta diretamente com o mecanismo de objeto do CA SDM (domsrvr). Toda a segurança do CA SDM, incluindo a partição de dados e as restrições de locação, é automaticamente aplicado aos relatórios, mas não ao seu ambiente de criação de relatórios. É possível configurar o ambiente de geração de relatório para que ele funcione com as partições de dados existentes no CA SDM.

  Observação: para obter informações sobre como estabelecer a segurança das partições de dados para seu ambiente de criação de relatório, consulte Como definir a segurança das partições de dados para a criação de relatórios (na página 836).

- **CMS (Central Management Server - Console de Gerenciamento Central)—** O repositório central que armazena todos os objetos usados nos processos de geração de relatório.

- **Central Management Console —** Um componente administrativo que fornece acesso a todas as funções de administração de BusinessObjects. Usando o CMC, você pode implementar relatórios e atribuir acesso de usuário e permissões de pasta para o InfoView. As opções de autenticação, funções e permissões de usuário devem ser estabelecidas pelo ambiente de criação de relatório com o uso do CMC (Central Management Console - Console de Gerenciamento Central).

  Observação: as opções de autenticação, funções e permissões de usuário devem ser estabelecidas pelo ambiente de criação de relatório antes de usar o CA Business Intelligence. Para obter mais informações sobre a definição da segurança, consulte Segurança e Autenticação (na página 836).

- **Universo do BusinessObjects—**Descreve as classes (tabelas) e objetos (colunas) que são usadas nos relatórios. O universo do CA SDM é instalado e configurado durante a instalação. Na conclusão da instalação, a conexão ao universo é atribuída a vários grupos e usuários no CA SDM.

- **Designer** — Um componente do BusinessObjects que permite modificar o Universo CA SDM, que é uma metacamada entre o esquema do CA SDM e as ferramentas de relatório do Business Objects. O Assistente de importação/exportação facilita o preenchimento ou extração dentro do CMS.

- **Relatórios predefinidos padrão** — Os relatórios predefinidos são relatórios do CA SDM e do Gerenciamento de conhecimento com base na web desenvolvidos com o Web Intelligence ou com o Crystal Reports. Os relatórios podem ser usados como modelos para definir relatórios específicos da localidade.

- **InfoView** — O BusinessObjects InfoView é uma interface web que permite que usuários autorizados do CA SDM interajam com relatórios predefinidos com base na web. É possível exibir, executar e programar tipos de relatório, inclusive, mas não apenas, do Web Intelligence e do Crystal Reports. Os relatórios são contidos em pastas na seção pública no InfoView.

- **Relatórios ad hoc—** Os relatórios ad hoc permitem a criação e a administração de relatórios usando a interface com base no plug-in do Web Intelligence. Esta ferramenta é destinada a usuários que queiram criar relatórios básicos facilmente sem a criação de consultas.

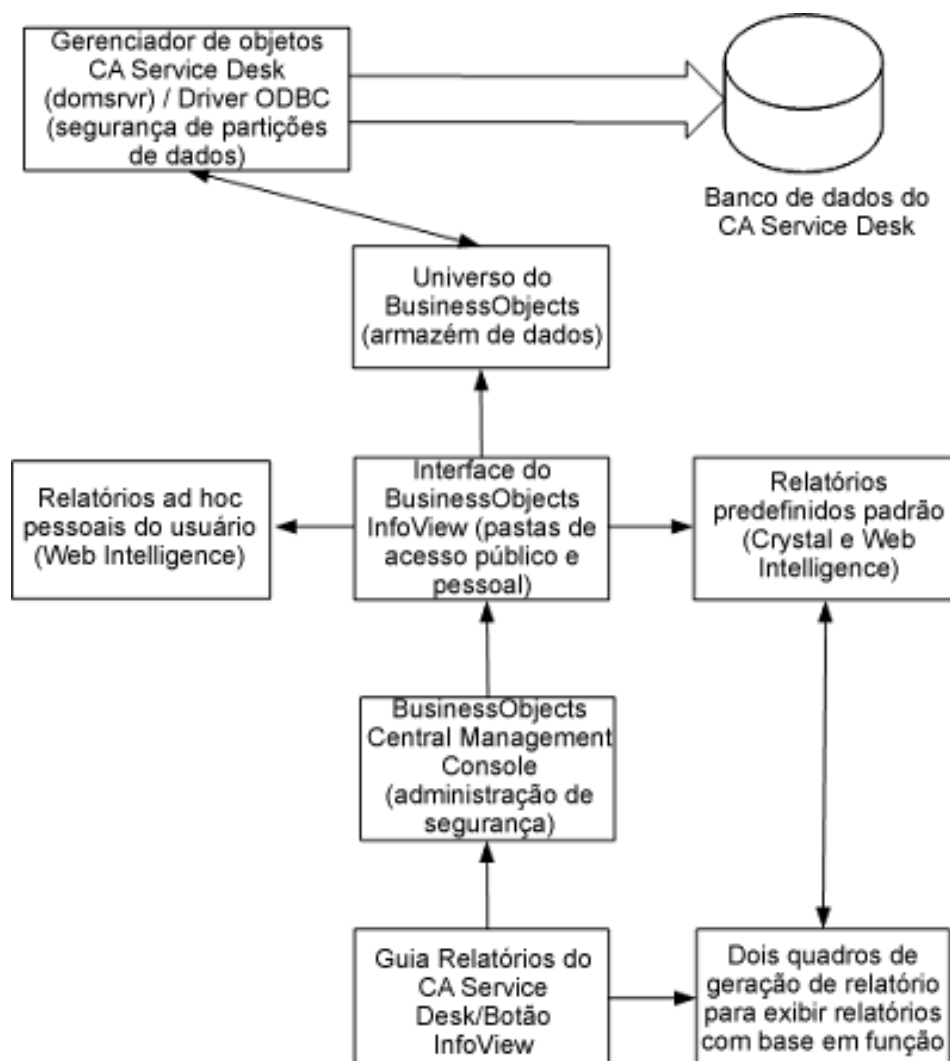
  Observação: para todos os exemplos de uso de relatório ad hoc, consulte Relatórios ad hoc (na página 873).

- **Relatórios de painel** — Os relatórios de painel permitem o monitoramento das operações diárias para todos os tipos de tickets do CA SDM (solicitação/incidente/problema, requisição de mudança ou ocorrência) no BusinessObjects InfoView. Cada relatório contém dados analíticos sobre aqueles com os melhores desempenhos no trabalho com tickets ativos, para que você possa monitorar seu progresso.

- **Guia Relatórios do CA SDM** — Na guia Relatórios do CA SDM, os usuários autorizados podem exibir relatórios com base em sua função e clicar no botão InfoView para gerenciar seus relatórios pessoais no InfoView.

  Observação: para obter informações sobre como gerenciar os relatórios com base em sua função e exibir novos relatórios na guia Relatórios, consulte Relatórios com base na web (na página 857).

Diagrama do fluxo de dados da geração de relatório

O diagrama abaixo ilustra o fluxo dos dados de componente e a execução para o CA Business Intelligence integrado ao BusinessObjects Enterprise:

Exibir relatórios no InfoView com base na web

O CA SDM usa a interface do BusinessObjects InfoView para coletar, organizar e apresentar informações em formatos de relatório.

Importante: Para todos os relatórios, você *deve* atualizar os campos Data para gerar relatórios. Os outros campos são opcionais.

Siga estas etapas:

1. Na guia Relatórios do CA SDM, clique no botão InfoView.

   A página inicial InfoView aparece.

2. No painel de Cabeçalho, selecione Lista de documentos.

   A Lista de documentos exibe relatórios do CA SDM, Ferramentas administrativas, amostras e assim por diante em pastas públicas. Quando você seleciona uma pasta, o conteúdo correspondente é exibido no painel de detalhes. As pastas que você pode acessar na lista de documentos depende dos direitos concedidos a você por seu administrador.

   Por exemplo, para exibir os relatórios do CMDB, navegue para CA Service Desk/CMDB. A lista de relatórios será exibida no painel de detalhes.

3. Clique duas vezes em um relatório.

   O formulário detalhado é exibido. O formulário contém os campos de entrada para gerar o relatório selecionado.

4. Digite as informações relevantes ao gerar o relatório selecionado.

   Exemplo: Se você abrir os ICs Adicionados no relatório do intervalo de tempo você precisa digitar o intervalo de tempo dentro do qual você deseja visualizar os ICs adicionados, os Nomes de inquilinos de IC e assim por diante.

   Importante: Se você estiver usando o banco de dados Oracle e deseja gerar Relatório de todos os impactos da mudança, o Relatório de relacionamentos de ICs, Relatório de análise de causa raiz e, em seguida, clique em Oracle (Esses relatórios funcionarão no Oracle apenas) da pasta do CMDB para acessar os relatórios. Se você gerar esses relatórios usando a pasta do SQL Server, os relatórios não serão gerados e será exibida uma mensagem de erro. Igualmente, se você estiver usando o banco de dados SQL e deseja gerar o Relatório de todos os impactos da mudança, o Relatório de relacionamentos de ICs, e o Relatório de análise da causa raiz, em seguida clique em SQL Server (Esses relatórios funcionarão somente no SQL Server) da pasta do CMDB para acessar os relatórios.

Observação: é obrigatório preencher todos os campos para gerar um relatório.

5. Clique em OK.

   O relatório aparece.

Observação: o BusinessObjects InfoView inclui um Guia do Usuário que descreve como usar o BusinessObjects InfoView. Para acessar o Guia do Usuário, clique no ícone de ajuda no InfoView.

Segurança e Autorização

A configuração de segurança padrão para o BusinessObjects Enterprise é realizada através da configuração CA Business Intelligence. A configuração determina as políticas de segurança de pastas, universos, conexões de universos e ferramentas. Ele também oferece métodos para adicionar usuários e mapeá-los para os grupos e configurar algumas opções de preferência.

Especificamente, a configuração de criação de relatórios do CA Business Intelligence envolve:

- Configurando a segurança
- Implementando relatórios
- Implementando universos
- Configurando os ajustes do Web Intelligence

Após a conclusão da instalação, a conexão do universo é atribuída a diversos grupos e usuários no CA SDM.

O administrador pode efetuar logon no CMC BusinessObjects e modificar a configuração padrão em qualquer ocasião. Os usuários são autorizados a acessar o InfoView com base no grupo CA Business Intelligence ao qual pertencem.

Grupos e usuários

Os grupos relacionados na tabela abaixo serão adicionados ao CMS (Central Management Server) durante a configuração do CA Business Intelligence. Eles estão relacionados às funções do CA SDM com os mesmos nomes. Durante a fase de configuração, uma caixa de seleção opcional é disponibilizada para indicar se os usuários de exemplo devem ser adicionados ao CMS. Caso ela seja selecionada, a configuração padrão de CMS inclui um usuário de exemplo para cada grupo. No CMC, é possível usar esses usuários de exemplo como modelos ao definir as permissões de usuário e opções de autenticação para seu ambiente de geração de relatórios.

Nome do grupo	Nome de usuário
Gerenciador de mudanças	Usuário do gerenciador de mudanças
Gerenciador de atendimento ao cliente	Usuário do gerenciador de atendimento ao cliente
Gerente de conhecimento	Usuário do gerente de conhecimento
Knowledge Analyst	Usuário do analista de conhecimento
Service Desk Manager	Usuário do Service Desk Manager
Gerente de incidentes	Usuário do gerenciador de incidentes
Gerenciador de problemas	Usuário do gerenciador de problemas

Partição de dados do CA SDM no InfoView

Considere as seguintes informações sobre os relacionamentos entre as partições de dados do CA SDM, e InfoView:

- O analista se conecta ao CA Business Intelligence por meio da guia Relatórios do CA SDM ou no InfoView com o tipo de acesso de um de função padrão do sistema de geração de relatórios.
- As credenciais de logon do CA SDM *devem* corresponder às credenciais do InfoView. O administrador define um método de autenticação, como secLDAP ou SecEnterprise. O CA SDM registra no CA Business Intelligence, que, em seguida, efetua logon no CA SDM por meio do ODBC.
- O logon do analista do CA Business Intelligence associa-se ao logon do CA SDM. CA Business Intelligence usa esse logon do CA SDM e a função de geração de relatórios associada com o tipo de acesso de logon. Se o analista não possui um logon do CA SDM associado, o CA Business Intelligence usa o padrão do sistema. O padrão do sistema é definido nos Parâmetros ODBC no Universe Designer e a função de geração de relatórios do tipo de acesso.
- Para restringir um usuário de visualizar um relatório, o administrador pode desativar o acesso ao relatório ou à pasta que o contém.

Universo e Conexões do Universo

A configuração padrão também inclui a política de segurança para acessar o universo CA SDM e as conexões do universo. Para permitir o acesso total, todos os grupos padrão são definidos para possuírem o acesso com Controle total

Nome do grupo	**Nível de acesso**
Gerenciador de mudanças	Controle total
Gerenciador de atendimento ao cliente	Controle total
Analista de conhecimento	Controle total
Gerente de conhecimento	Controle total
Service Desk Manager	Controle total
Gerente de incidentes	Controle total
Gerenciador de problemas	Controle total

Pasta de Relatórios

A configuração padrão possui um conjunto de pastas contendo relatórios predefinidos para o CA SDM e Gerenciamento de conhecimento. Cada grupo CA SDM é configurado para ter acesso a um subconjunto dessas pastas.

Nome da pasta	Nome do grupo	Nível de acesso
Agregado	■ Gerenciador de mudanças ■ Gerenciador de atendimento ao cliente ■ Gerente de conhecimento ■ Analista de conhecimento ■ Service Desk Manager ■ Gerente de incidentes ■ Gerenciador de problemas	■ Exibir ■ Exibir ■ Sem acesso ■ Sem acesso ■ Controle total ■ Exibir ■ Exibir
Ativo	■ Gerenciador de mudanças ■ Gerenciador de atendimento ao cliente ■ Gerente de conhecimento ■ Analista de conhecimento ■ Service Desk Manager ■ Gerente de incidentes ■ Gerenciador de problemas	■ Exibição sob demanda ■ Exibir ■ Sem acesso ■ Sem acesso ■ Controle total ■ Exibir ■ Exibir
Requisição de mudança (inclui todas as subpastas)	■ Gerenciador de mudanças ■ Gerenciador de atendimento ao cliente ■ Gerente de conhecimento ■ Analista de conhecimento ■ Service Desk Manager ■ Gerente de incidentes ■ Gerenciador de problemas	■ Controle total ■ Sem acesso ■ Sem acesso ■ Sem acesso ■ Exibir ■ Exibir ■ Exibir

Nome da pasta	Nome do grupo	Nível de acesso
Ocorrência (inclui todas as subpastas)	■ Gerenciador de mudanças	■ Sem acesso
	■ Gerenciador de atendimento ao cliente	■ Controle total
	■ Gerente de conhecimento	■ Sem acesso
	■ Analista de conhecimento	■ Sem acesso
	■ Service Desk Manager	■ Sem acesso
	■ Gerente de incidentes	■ Sem acesso
	■ Gerenciador de problemas	■ Sem acesso
Solicitação (inclui todas as subpastas)	■ Gerenciador de mudanças	■ Sem acesso
	■ Gerenciador de atendimento ao cliente	■ Sem acesso
	■ Gerente de conhecimento	■ Sem acesso
	■ Analista de conhecimento	■ Sem acesso
	■ Service Desk Manager	■ Controle total
	■ Gerente de incidentes	■ Exibir
	■ Gerenciador de problemas	■ Sem acesso
Gerenciamento de conhecimento	■ Gerenciador de mudanças	■ Sem acesso
	■ Gerenciador de atendimento ao cliente	■ Exibir
	■ Gerente de conhecimento	■ Controle total
	■ Analista de conhecimento	■ Exibir
	■ Service Desk Manager	■ Cronograma
	■ Gerente de incidentes	■ Exibir
	■ Gerenciador de problemas	■ Exibir
Pesquisa	■ Gerenciador de mudanças	■ Sem acesso
	■ Gerenciador de atendimento ao cliente	■ Sem acesso
	■ Gerente de conhecimento	■ Exibir
	■ Analista de conhecimento	■ Sem acesso
	■ Service Desk Manager	■ Controle total
	■ Gerente de incidentes	■ Exibir
	■ Gerenciador de problemas	■ Exibir

Nome da pasta	Nome do grupo	Nível de acesso
Gerenciamento de incidentes e problemas	■ Gerenciador de mudanças ■ Gerenciador de atendimento ao cliente ■ Gerente de conhecimento ■ Analista de conhecimento ■ Service Desk Manager ■ Gerente de incidentes ■ Gerenciador de problemas	■ Sem acesso ■ Sem acesso ■ Exibir ■ Sem acesso ■ Cronograma ■ Controle total ■ Controle total

Níveis de Acesso

A configuração padrão inclui os seguintes níveis de acesso para os grupos e usuários:

Sem acesso

Define todas as permissões para Não especificado.

Exibir

Permite que o usuário visualize a pasta, o relatório ou o universo. Se o relatório contém dados, o usuário pode abrir e interagir com ele. Caso o relatório não contenha dados, o usuário não pode atualizá-lo. Por padrão, o usuário pode editar o relatório e salvá-lo em uma pasta pessoal e atualizá-lo lá. É possível evitar explicitamente que os usuários copiem documentos corporativos para pastas pessoais ao definir um direito individual que negue a "Cópia de objetos para outra pasta".

Cronograma

Permite que o usuário programe um relatório, mas não o atualiza em tempo real.

Exibição sob demanda

Permite que o usuário atualize um relatório em tempo real. Quando o relatório é um documento do Web Intelligence, o usuário também precisa do acesso à Exibição sob demanda do universo e da conexão com o universo para realizar a atualização.

Controle total

Permite que o usuário crie novos relatórios em uma pasta, modifique os relatórios existentes ou exclua itens.

Avançado

Quando os níveis de acesso anteriores não atenderem suas necessidades, é fornecido o acesso mais granular ao selecionar a opção Avançado.

Quando o nível de acesso do grupo ou do usuário está definido para Avançado, é disponibilizado um controle mais granular de direitos do que o atribuído através da seleção de Exibir cronograma, Exibição sob demanda ou Controle total.

As pastas do BusinessObjects usam a segurança herdada. A autoridade recebida é a mesma em pastas de nível mais baixo e em pastas de nível superior atribuída a você ou seu grupo, a menos que sejam aplicadas restrições imperativas em níveis inferiores. As autorizações padrão são fornecidas no nível da pasta e no nível do grupo. Os usuários irão herdar os direitos de seu grupo para todos os objetos na pasta e pastas secundárias.

O CA Business Intelligence é instalado com dois grupos: Administradores e Todos. O grupo Todos recebe um Nível de acesso de programação que permite a programação e a exibição de todos os objetos de relatório.

Mais informações:

Pasta de Relatórios (na página 839)

Como apontar um servidor do CA Business Intelligence para um servidor do CA SDM

Caso possua um servidor CA Business Intelligence existente, é possível apontá-lo para um servidor do CA SDM da seguinte maneira:

1. Criar uma nova origem de dados ODBC. (na página 843)
2. Configurar o universo (na página 844).
3. Exportar o universo. (na página 844)
4. Executar o InfoView para verificar a conexão.

Criar uma origem de dados ODBC

Você pode criar uma origem de dados ODBC usando o Administrador de fonte de dados ODBC.

Para criar uma origem de dados ODBC

1. Navegue até Iniciar, Todos os programas, Ferramentas administrativas, Fontes de dados (ODBC).

   O Administrador da origem de dados ODBC é exibido.

2. Selecione a guia DSN do sistema e clique em Adicionar.

   A página Criar nova origem de dados é exibida.

3. Selecione DataDirect OpenAccess e clique em Concluir.

   A página DataDirect OpenAccess ODBC Setup é exibida.

4. Especifique o casd_*servername* no campo ODBC Name.
5. Clique em Avançado.

   A página Avançado é exibida.

6. Clique em Adicionar.

   A página Open Access Database Setup é exibida.

7. Preencha os seguintes campos:
   - **Nome**. Especifique o casd_*servername*.
   - **Endereço IP**. Especifique o *servername* ou o endereço IP.

     Observação: efetue o ping com o *servername* para determinar seu endereço IP para usá-lo em vez de o *servername*.

   - **Porta**. Especifique 1706.
   - **Tipo**. (Opcional) Especifique o banco de dados usado no servidor. Esse campo é usado apenas como informação de referência.
8. Clique em OK.
9. Selecione casd_*servername* na lista suspensa Banco de dados.
10. Clique em OK.

    A origem de dados ODBC é criada.

Configurar o universo

Após criar a origem de dados ODBC, é necessário configurar o universo ao estabelecer uma conexão entre o CA SDM e o CA Business Intelligence.

Para configurar o universo

1. Execute o Designer e efetue o logon como administrador.
2. Clique em Arquivo, Importar.

   A página Import Universe é exibida.
3. Navegue e selecione seu universo CA SDM e clique em OK.

   A mensagem Universe successfully imported é exibida.
4. Clique em Arquivo, Parâmetros.

   A página Universe Parameters aparece.
5. Clique em Editar.

   A página Editar conexão do CA SDM é exibida.
6. Especifique o nome de usuário e senha do usuário privilegiado do CA SDM, como o ServiceDesk.
7. Selecione casd_*servername* a partir do nome da origem de dados e clique em Avançar.
8. Clique em Testar conexão para verificar se o universo do CA SDM se comunica com o CA Business Intelligence.
9. Clique em Avançar, Avançar e em Concluir.

   O universo é configurado.

Exportar o universo

Após configurar o universo, ele deve ser exportado do Designer.

Para exportar o universo

1. Clique em Arquivo, Exportar.

   A caixa de diálogo Exportar Universo aparece.
2. Clique em Continuar.
3. Clique em OK.

   O universo é exportado

Como definir a segurança de partições de dados para a geração de relatórios

O acesso à geração de relatório do CA Business Intelligence é restrito pela segurança de partição de dados do CA SDM. Toda a segurança do CA SDM, inclusive partição de dados e restrições de locação, é automaticamente aplicada aos relatórios.

A segurança da partição de dados para seu ambiente de geração de relatórios específico não é aplicada durante a fase de configuração. Configure o ambiente de geração de relatório para que ele funcione com as partições de dados existentes no CA SDM.

Use as ferramentas a seguir para realizar esta tarefa:

- **BusinessObjects Central Management Console** (CMC)— Permite a administração da autenticação e das permissões do BusinessObjects Enterprise.
- **BusinessObjects Designer**—Permite modificar o universo para o CA SDM, Gerenciamento de conhecimento, CMDB e Support Automation que é uma metacamada entre o esquema CA SDM e as ferramentas de relatório.
- **CA SDM Security and Role Management**—Permite definir a segurança das partições de dados para determinar quais dados os usuários podem acessar.

Adicionar o usuário privilegiado do CA SDM ao CMC

A conexão do universo é configurada, por padrão, para usar o Usuário privilegiado e Senha do Service Desk ao acessar os dados. O usuário deve ser adicionado ao CMC como um novo usuário do CA Business Intelligence. Há duas finalidades na adição desse usuário. Primeiro, o usuário será necessário caso planeje definir a segurança da partição de dados para a geração de relatórios e segundo, ele permitirá a você usar esse usuário quando, inicialmente, testar os relatórios a partir da guia Relatórios do CA SDM. A guia Relatórios exige um usuário que esteja definido tanto para o CA SDM quanto CA Business Intelligence.

Use as instruções fornecidas no *Guia de Implementação* para adicionar os usuários CA SDM ao CMC e configurar a conta de Usuário privilegiado do CA SDM.

Definir as credenciais de banco de dados do universo

O universo deve usar as credenciais do banco de dados associadas à conta de usuário do BusinessObjects.

Observação: certifique-se de acessar o BusinessObjects Designer usando a conta de Usuário privilegiado e não a conta de Usuário administrador.

Para definir as credenciais de banco de dados do universo

1. No menu Iniciar, navegue até BusinessObjects XI, BusinessObjects Enterprise, Designer.
2. Faça logon no Designer.

   A janela Designer aparece.
3. Selecione Arquivo, Importar.

   A caixa de diálogo Import Universe será exibida.
4. Selecione a pasta CA SDM, Gerenciamento de conhecimento, CMDB, ou Support Automation Universes a partir da lista suspensa.

   Observação: caso essa seja a primeira vez que está usando o Designer, selecione Procurar, CA Universes.
5. Verifique o caminho do arquivo para a pasta de importação na caixa Import Folder.
6. Clique em OK.

   A janela universe aparece.
7. Selecione Arquivo, Parâmetros.

   A caixa de diálogo Universe Parameters aparece.
8. Na guia Definição, clique em Editar.

   A caixa de diálogo Parâmetros de login aparece.
9. Selecione as credenciais do banco de dados associada à caixa de seleção da conta do Business Objects.
10. Clique em Avançar, Testar conexão e espere até a conexão do universo aparecer.
11. Clique em OK para concluir.
12. Selecione Arquivo, Exportar.

    A caixa de diálogo Export Universe aparece.

13. Selecione o universo que deseja usar a partir da lista suspensa Domínio.
14. Selecione Todos da lista de Grupos
15. Clique em OK para exportar as mudanças no universo.

Estabelecer partições de dados

No Gerenciamento de segurança e função, crie uma constrição de partição de dados que irão restringir o acesso ao registro do banco de dados para todos os usuários de relatório atribuídos à partição de dados.

Observação: para obter informações sobre as constrições de partições de dados, consulte Configuração das partições de dados (na página 204).

Banco de dados replicado para geração de relatórios offline

Para gerenciar potenciais problemas de desempenho que possam afetar os componentes de geração de relatório instalados com o CA SDM, é possível criar um banco de dados replicado para finalidades de geração de relatórios offline.

Observação: para obter mais informações sobre criação de um banco de dados replicado para geração de relatórios offline, consulte a documentação de exemplo e scripts fornecidos no diretório NX_ROOT\samples\reporting.

Relatórios de Role-Based

O CA SDM apresenta relatórios com base em funções em dois quadros de geração de relatório na guia Relatórios. Cada quadro fornece exibições gráficas que permitem que o usuário faça uma busca detalhada nos dados do relatório para mostrar os dados cobertos pelos gráficos e grupos resumidos. Você pode gerenciar relatórios com base em funções e exibir novos relatórios do BusinessObjects na guia Relatórios.

A página Lista de relatórios contém detalhes dos relatórios disponíveis para uso. Clique no ícone Lista de relatórios no quadro selecionado para exibir essa página.

Definir relatórios com base na função para a função

É possível gerenciar os formulários da web de relatórios que são exibidos na página da Lista de relatórios quando um usuário atribuído a essa função efetua o logon no sistema.

Para definir um relatório com base na função para a função

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Lista de funções.

   A página Lista de funções aparece. As seguintes funções padrão estão disponíveis para Relatar:

   - Gerenciador de mudanças
   - Gerenciador de atendimento ao cliente
   - Gerente de conhecimento
   - Knowledge Analyst
   - Service Desk Manager
   - Gerente de incidentes
   - Gerenciador de problemas

2. Selecione *uma* das funções Relatar na lista.

   A página Role Detail Form é exibida. Essa página contém as seguintes guias:

   Autorização

   Permite definir o nível de autorização atribuído à função.

   Acesso a funções

   Define o acesso de função a cada área funcional do CA SDM.

   Interface web

   Personaliza a interface web para a função, definindo as páginas da web e o conteúdo da ajuda online que os usuários podem acessar.

   Gerenciamento de conhecimento

   Especifica os privilégios de Gerenciamento de conhecimento para a função.

   Visibilidade do documento KT

   Especifica quais status do documento a função está autorizada a visualizar (por exemplo, rascunho, desativado e publicado).

Guias

Define as guias que aparecem quando um usuário atribuído a esta função faz logon no CA SDM.

Formulários web de relatório

Define os formulários web de relatório que estão disponíveis para esta função.

Recursos Ir

Especifica quais tipos de registro aparecerão na lista suspensa "Ir" para a função. Na página Detalhe da função, selecione a guia Formulários web de relatório.

3. Clique na guia Formulários web de relatório.

   A página Lista de formulários web de relatório é exibida. A página contém detalhes sobre relatórios disponíveis para uso.

4. Clique em Atualizar formulário web.

   A página Pesquisa de formulário web aparece.

5. Insira critérios de pesquisa para exibir os formulários web e clique em Pesquisar.

   A página Atualização de formulários web atribuídos aparece, listando os formulários correspondentes aos critérios de pesquisa.

6. Na lista na esquerda, selecione os formulários web que você quer exibir para esta função. Para selecionar vários itens, mantenha pressionada a tecla CTRL enquanto clica com o botão esquerdo do mouse.

7. Após selecionar todos os formulários que você quer, clique no botão Selecionar.

   Os formulários selecionados passam para a lista Formulários web atribuídos da direita.

8. Clique em OK.

   A página Detalhes da função aparece, com os formulários web selecionados listados na guia Formulários web de relatório.

Exibir novos relatórios na guia Relatórios

Quando um relatório é aprovado para uso dentro do CA SDM, ele é movido para a seção pública do InfoView, tornando-se disponível para usuários autorizados. Para adicionar o relatório ao CA SDM, o administrador deve realizar algumas etapas adicionais.

Você pode exibir novos relatórios criados no CA Business Intelligence na guia Relatórios do CA SDM. Use as ferramentas a seguir para realizar esta tarefa:

- Pintor de telas da web
- Gerenciamento de funções

Antes de começar, faça o seguinte:

- Instale e configure o CA Business Intelligence para trabalhar com o CA SDM.

  Observação: para obter informações sobre a instalação, consulte o *Guia de Implementação* e o *Guia de Instalação do CA Business Intelligence*.

- Estabeleça permissões de usuário, funções e opções de autenticação (na página 836) para seu ambiente de geração de relatório.

Etapa 1: Criar dois registros de formulário da web para chamar os novos relatórios

Por padrão, a guia Relatórios contém dois quadros de relatório que permitem que os usuários autorizados exibam os novos relatórios. Nessa etapa, você irá criar dois registros de formulário da web e irá definir os URLs que apontam para os novos relatórios.

Para criar dois registros de formulário da web para chamar os relatórios

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Formulários web.

   A página da Lista de formulários web aparece.

2. Clique em Criar novo.

   A página Criar formulário web aparece.

3. Preencha os seguintes campos:

   Nome do formulário web

   Especifique o nome que identifica o formulário web. Esse é um campo obrigatório.

   Exemplo: Relatório da lista de ativos

Status do registro

Especifique ativo.

Código

Especifique o valor do código exclusivo que identifica o formulário web para o sistema. Após definido, o código não pode ser alterado.

Exemplo: asset_list

Observação: faça uma anotação do valor inserido no campo Código.

Tipo

Selecionar relatório.

Descrição

(Opcional) Insira uma breve descrição do formulário web.

Recurso

Especifique o URL que chama o novo relatório.

Exemplo: Abra o formulário da web de Lista de ativos a partir da lista de Formulários da web no Gerenciamento de função e especifique o URL exibido nesse formulário.

```
$BOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk]
,[Asset]&sDocName=Asset+List&sViewer=html
```

4. Clique em Salvar.

   A definição de formulário web é salva e a página Detalhes do formulário web aparece.

5. Repita as etapas de 1 a 3 para criar um segundo registro de formulário da web que irá chamar o segundo URL de relatório. Faça uma anotação do valor inserido no campo Código.

Etapa 2: Criar uma página de múltiplos quadros e atribuir os novos relatórios

No Pintor de telas da web, crie uma página da web de múltiplos quadros chamada Frameset. Então, atribua os registros de formulário da web criados na etapa 1 a esse Frameset.

Observação: é possível criar essa página com qualquer quantidade de quadros. Esteja ciente de que adicionar quadros adicionais limitará a visibilidade na guia Relatórios.

Para criar uma página com múltiplos quadros e atribuir os relatórios

1. No Pintor de telas da web, selecione Arquivo, Novo.

   A caixa de diálogo Novo formulário é exibida.

2. Preencha a interface e os campos do grupo do formulário apropriadamente.
3. Selecione multiframe.template a partir da lista Nome do arquivo.
4. Clique em Novo.

   A janela multiframe.htmpl é exibida.

5. Selecione Controles, Inserir Frameset.

   A caixa de diálogo Inserir frameset é exibida.

6. Não altere as configurações e clique em OK.

   São exibidos dois quadros verticais no Frameset.

7. Clique com o botão direito do mouse no quadro vertical da esquerda e selecione Propriedades no menu de atalho.

   A caixa de diálogo Properties - Frameset é exibida.

8. Selecione o campo em branco próximo ao atributo web_form_name e clique no botão (...).

   A caixa de diálogo Digitar nome do formulário web aparece.

9. Especifique o valor do código do primeiro relatório.

   Exemplo: asset_list

10. Após o nome do formulário da web do relatório ser encontrado, clique em Validar.
11. Clique com o botão direito do mouse no quadro vertical, especifique o valor do código do segundo relatório e valide o relatório.
12. Salve a página multiframe.htmpl. Anote o nome desse arquivo.

    Exemplo: report_mframe.htmpl

13. Selecione Arquivo, Publicar.

    A publicação faz com que os formulários sejam disponibilizados para todos os usuários do CA SDM. Para a função Analista, o arquivo está disponível no seguinte local: Arquivos de Programas/CA/Service Desk/Site/mods/www/htmpl/web/analyst/report_mframe.htmpl.

    Observação: ao pesquisar os formulários da web com múltiplos quadros no CA SDM, navegue até Gerenciamento da segurança e das funções, Gerenciamento de função, Formulários da web na guia Administração. Essa coluna especifica o web_form_name na guia Propriedades para um formulário de quadros múltiplos no Pintor de telas da web.

Etapa 3: Criar uma página inicial para a guia Relatórios

No Gerenciamento de função, crie uma página inicial para chamar a página da web com múltiplos quadros criada na Etapa 2.

Para criar uma página inicial para a guia Relatórios

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Formulários web.

   A página da Lista de formulários web aparece.

2. Clique em Criar novo.

   A página Criar formulário web aparece.

3. Preencha os seguintes campos:

   Nome do formulário web

   Especifica o nome que identifica um formulário web. Esse campo é obrigatório.

   Exemplo: página inicial

   Status do registro

   Especifica ativo ou inativo.

   Código

   Especifica o valor do código exclusivo que identifica o formulário web para o sistema. Após definido, o código não pode ser alterado.

   Exemplo: start_page

Tipo

Especifica HTMPL.

Descrição

(Opcional) Especifica uma breve descrição do formulário web.

Recurso

Especifica o URL que chama o novo relatório.

Exemplo: selecione o registro do Reports Multiframe do administrador na página Lista de formulários da web. Especifique o URL que aparece neste formulário. No final desse caminho, especifique a nova página de múltiplos quadros (report_mframe.htmpl).

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=report_mframe.htmpl
```

Clique em Salvar.

O novo registro da página inicial é exibido na página Lista de formulários da web.

Etapa 4: Criar um Registro da guia relatórios e atribuir Página inicial

No Gerenciamento de função, crie uma nova guia Relatórios e especifique a página inicial criada na etapa 3.

Para criar uma guia e atribuir a página inicial que chama os relatórios

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Guias na guia Administração.

   A página Lista de guias aparece.

2. Clique em Criar novo.

   A página Criar guia aparece.

3. Preencha os seguintes campos:

   Nome da guia

   Especifique o nome que identifica a guia dentro da interface administrativa. Por exemplo, o nome da guia aparece na página Lista de guias.

   Exemplo: Guia Relatórios

Código

Especifique o código que identifica a guia para o sistema. Após definido, o código não pode ser alterado.

Exemplo: reports_tab

Status do registro

Especifique ativo.

Nome de exibição

Especifique o nome que aparece na apresentação gráfica da guia na interface de usuário.

Exemplo: Guia Relatórios

Página inicial

Especifique o formulário web inicial que aparece na janela principal quando um usuário seleciona essa guia.

Exemplo: página inicial

4. Clique em Salvar.

   O formulário é exibido na página Lista de formulário da web.

Etapa 5: atribuir o Registro da guia a um Registro de função

No Gerenciamento de função, atribua a guia Relatórios à função listada desejada na página de Detalhe da função. Quando um usuário atribuído a essa função efetua o logon no sistema, ele verá a nova guia Relatórios na interface da web.

Para atribuir o Registro da guia a um registro de função

1. Selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Lista de funções na guia Administração.

   A página Lista de funções aparece.

2. Selecione a função desejada na lista Função.

   A página Detalhes da função aparece.

3. Na parte inferior dessa página, selecione Guias, e Atualizar guias.

   A nova guia aparece na guia Lista.

Criar uma página inicial para o botão InfoView

É possível ainda inserir o botão do InfoView que abre o BusinessObjects InfoView em uma nova janela na guia Relatórios. Essa opção é controlada pela opção de Página inicial que aparece no registro da guia Relatórios.

Para criar uma página inicial para o botão InfoView

1. Na guia Administração, navegue para Gerenciamento da segurança e das funções, Gerenciamento de funções, Formulários web.

   A página da Lista de formulários web aparece.

2. Clique em Criar novo.

   A página Criar formulário web aparece.

3. Preencha os seguintes campos:

   Nome do formulário web

   (Obrigatório) Especifica o nome que identifica um formulário web.

   Exemplo: página do InfoView

   Status do registro

   Especifica ativo ou inativo.

   Código

   Especifica o valor do código que identifica o formulário web para o sistema.

   Exemplo: info_view_page

   Tipo

   Especifica HTMPL.

   Descrição

   (Opcional) Descreve o formulário web.

   Recurso

   Especifica o URL que chama os quadros de relatório.

Exemplo: selecione o registro do InfoView do administrador na página Lista de formulários da web. Especifique o URL que aparece neste formulário. No final desse caminho, especifique a nova página inicial da guia Relatórios (start_page).

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=show_report_frames.ht
mpl+KEEP.report_form=start_page
```

Clique em Salvar.

A página inicial do InfoView é exibida na página Lista de formulários da web.

Etapa 7: atribuir a página inicial do botão InfoView ao registro na guia Relatórios

No Gerenciamento de função, atribua a página inicial do botão do InfoView criada na etapa 6 ao registro da guia Relatórios.

Para atribuir a página inicial do botão InfoView ao registro na guia Relatórios

1. Selecione o novo registro de formulário da guia Relatórios na página Lista da guia no Gerenciamento da função.

   A página detalhe aparece.

2. Selecione Editar.

   A página Atualizar guia aparece.

3. Especifique a página inicial do botão InfoView no campo Página inicial.
4. Clique em Salvar.

   Quando o usuário abre a guia Relatórios, o botão InfoView é exibido no canto superior direito do formulário.

Relatórios com base na web

O CA Business Intelligence instala um conjunto de relatórios predefinidos com base na web para o CA SDM e o Gerenciamento de conhecimento. Eles são desenvolvidos com o BusinessObjects Enterprise Web Intelligence ou com o Crystal Reports. Os relatórios podem ser usados como modelos para definir relatórios específicos da localidade.

Esses relatórios estão contidos em pastas que são automaticamente implementadas no servidor de criação de relatórios do CA Business Intelligence após a instalação.

É possível atribuir segurança a pastas e documentos para especificar se eles podem ser acessados globalmente, por funções específicas ou por indivíduos.

Observação: o BusinessObjects InfoView inclui um Guia do Usuário que descreve como usar o BusinessObjects InfoView. Para acessar o Guia do Usuário, clique no ícone de ajuda no InfoView. *Observação:* para obter informações gerais sobre o uso de relatórios predefinidos, consulte a Ajuda online.

Mais informações:

Interface do BusinessObjects InfoView (na página 858)
Navegar para relatórios (na página 858)
Preferências do InfoView (na página 859)
Relatórios de programação (na página 859)
Configuração da análise de dados (na página 860)
Publicar e distribuir relatórios (na página 861)

Interface do BusinessObjects InfoView

Na guia Relatórios do CA SDM, analistas e gerentes podem trabalhar com relatórios definidos para sua função ou gerenciar seus relatórios pessoais clicando no botão InfoView. No InfoView, os usuários podem acessar documentos do Web Intelligence e do Crystal Reports, além de outros objetos, e organizá-los de acordo com suas preferências.

Os recursos disponíveis no InfoView variam por tipo de conteúdo, mas, em geral, o usuário pode exibir informações no navegador da web, exportá-las para outros aplicativos comerciais (como o Microsoft Excel) e salvá-las em um local especificado.

Observação: as pastas e os objetos que os usuários podem ver no InfoView dependem da atribuição do seu grupo (função).

Navegar para relatórios

É possível navegar para as pastas na seção esquerda da janela InfoView para exibir, programar, modificar ou executar o relatório, ou para exibir o histórico e as propriedades de um relatório.

Para exibir um relatório

1. Use *um* dos métodos a seguir para abrir o InfoView:
   - Na guia Relatórios do CA SDM, clique no botão InfoView.
   - No menu Iniciar, navegue até Todos os programas, BusinessObjects XI, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.

   A página inicial InfoView aparece.
2. Na seção esquerda, navegue na estrutura da pasta Public Folders/CA Reports/CA SDM.
3. Clique na pasta correspondente ao tipo de relatório que você quer exibir.
4. Clique no nome do relatório para o tipo de informações que você quer consultar.

   O relatório aparece no BusinessObjects InfoView.

Preferências do InfoView

Os usuários podem definir preferências gerais para especificar se o InfoView deve iniciar com uma das páginas de painel pessoais criadas com a ferramenta My InfoView do Web Intelligence. Eles podem também definir suas preferências pessoais de exibição do Web Intelligence e do Crystal Reports.

Relatórios de programação

O InfoView oferece suporte à programação dos relatórios. Para a geração de relatórios ad-hoc, os relatórios programados são armazenados na seção My Folders. Se um relatório estiver configurado para "refresh on open", o sistema irá acessar o banco de dados para obter as informações mais recentes sempre que o usuário final visualizar o relatório. Os usuários podem programar os relatórios para serem executados em determinados momentos.

Os administradores podem definir os calendários para refletir as datas de programação adequadas. Por exemplo, um usuário pode selecionar um calendário usando a opção "Quando" (para o tempo e a frequência), ao fazer isso, serão exibidos os dias úteis disponíveis e o restante dos dias será ignorado.

Observação: para obter mais informações sobre a programação de relatórios, consulte a documentação do BusinessObjects.

Com a programação, os usuários podem:

- Especificar o tempo e a frequência da programação (agora, de hora em hora, diariamente e semanalmente, por exemplo).
- Especificar o destino, como uma caixa de entrada, local do arquivo ou destinatário do e-mail.
- Indicar para quais caixas de entrada o relatório deve ser enviado.
- Especificar a saída do relatório, como o Web Intelligence, Crystal Report, Microsoft Excel e Adobe Acrobat.
- Especificar opções de armazenamento em cache. Por padrão, os resultados dos documentos são armazenados no Output File Repository Server. Os usuários podem optar por ter o relatório no cache do sistema no Web Intelligence Report Server ao selecionar um formato e local para o armazenamento em cache.
- Selecione um grupo de servidor para processar uma solicitação. Se um evento definido for selecionado, o objeto será executado apenas quando a condição adicional ou evento ocorrer.

Observação: se as partições de dados CA SDM forem usadas para gerenciar as restrições de dados na seção da pasta pública do InfoView, os relatórios programados contidos em pastas públicas devem ser definidas para cada usuário.

Configuração da análise de dados

Um visualizador interativo fornece um conjunto extenso de ferramentas para ajustar o modo de exibição dos dados do relatório. Você pode fazer uma busca detalhadas em vários níveis, como o grupo, o responsável ou as solicitações reais.

Os visualizadores interativos permitem fazer o seguinte:

- Alterar a aparência do relatório, apresentando os dados em um formato de "bloco" diferente, como um gráfico de pizza. Por exemplo, clicar com o botão direito do mouse no relatório e selecionar "Turn table to" exibe recursos de apresentação de relatório.
- Executar tarefas diferentes, como classificar, criar quebras de relatório, calcular, filtrar e classificar o relatório.
- Compartilhar informações com outros usuários e grupos.

Publicar e distribuir relatórios

Os usuários do InfoView podem salvar dados do relatório em formato de Excel, PDF ou CSV, e distribuí-lo a um local de arquivo, uma caixa de entrada, um endereço de email ou site de FTP.

Quando um relatório é aprovado para uso dentro do CA SDM, ele é movido para a seção pública, tornando-se disponível para usuários autorizados. É possível atribuir segurança a pastas e documentos para especificar se eles podem ser acessados globalmente, por funções específicas ou por indivíduos. A segurança é administrada no BusinessObjects Central Management Console.

Principais indicadores de desempenho

Os *Indicadores principais de desempenho* (KPIs) são métricas que você pode usar para identificar áreas de seu ambiente de gerenciamento de serviço que possam exigir atenção administrativa ou ajuste da configuração.

Use a interface da web do CA SDM para configurar suas definições de KPI. Os dados que eles produzem são armazenados no banco de dados do CA SDM e estão disponíveis para a produção de relatórios com base na web (na página 857).

Observação: além de definir as consultas de KPI, é possível configurar o daemon de KPI para recuperar os dados do ticket do CA SDM sempre que um ticket é aberto, fechado ou alguns campos são modificados.

Com a definição e o monitoramento de um conjunto planejado de KPIs, você pode mensurar o progresso em direção às metas de desempenho de sua organização e reunir dados valiosos para orientar decisões estratégicas sobre seu ambiente de TI.

Observação: para obter informações sobre tabelas de banco de dados de KPI, consulte o *Guia de Referência Técnica*.

Tipos de KPI

O CA SDM oferece suporte a três tipos de KPI:

- **KPIs de sistema** são instalados com o produto. É possível personalizá-los para atender a suas necessidades, mas não pode criar novos KPIs de sistema.

- **KPIs de consulta armazenada** invocam a consulta armazenada para recuperar métricas do banco de dados. É possível criar KPIs de consulta armazenada personalizados ou modificar os exemplos predefinidos instalados com o produto.
- **KPIs de SQL** permitem incorporar uma consulta completa do SQL diretamente no KPI. É possível criar KPIs de SQL personalizados ou modificar os exemplos predefinidos instalados com o produto.

Observações:

- Para obter detalhes sobre a configuração dos três tipos de KPI, consulte a *Ajuda on-line*.
- Os KPIs, predefinidos ou criados pelo usuário, não podem ser excluídos. Quando o KPI não for mais necessário, é possível desativá-lo ao definir o Status do registro como inativo.

KPIs predefinidos

São instalados diversos KPIs de cada tipo com o CA SDM. Pode ser útil examiná-los ao ler esse guia.

É possível usar os KPIs SQL e de consulta armazenadas com suas definições originais ou como modelos para as definições personalizadas.

É possível também usar os KPIs do sistema com as definições originais ou modificar alguns campos para atender suas necessidades.

Observação: a maioria dos KPIs predefinidos são configurados como inativos por padrão. Para visualizá-los na interface da web, filtre a página de Lista de KPIs para exibir os KPIs inativos.

Daemon do Indicador Principal de Desempenho

O daemon de KPI gerencia a recuperação, organização e armazenamento dos dados de métrica do KPI. O daemon é executado continuamente e coleta dados em intervalos de tempo especificados a partir de diversos recursos do sistema.

Quando o horário de atualização de KPI chega, o daemon de KPI interage com os outros componentes do sistema da seguinte maneira:

- **KPI do sistema**—Envia uma solicitação para um daemon de destino (webengine, domsrvr, bpvirtdb ou db_agents) para recuperar a conta e os dados de duração.
- **KPI de consulta armazenada**—Envia uma solicitação para o domsrvr pra coletar os dados da conta.
- **KPI de SQLI**—Envia uma solicitação para o domsrvr para coletar os dados de duração, máx, soma ou conta.

Quando o daemon do KPI recebe os dados de solicitação, ele armazena as métricas resultantes no banco de dados.

Observação: A duração calculada é baseada em uma mudança de valores em um ticket em tempo real, não no horário comercial.

KPIs de sistema

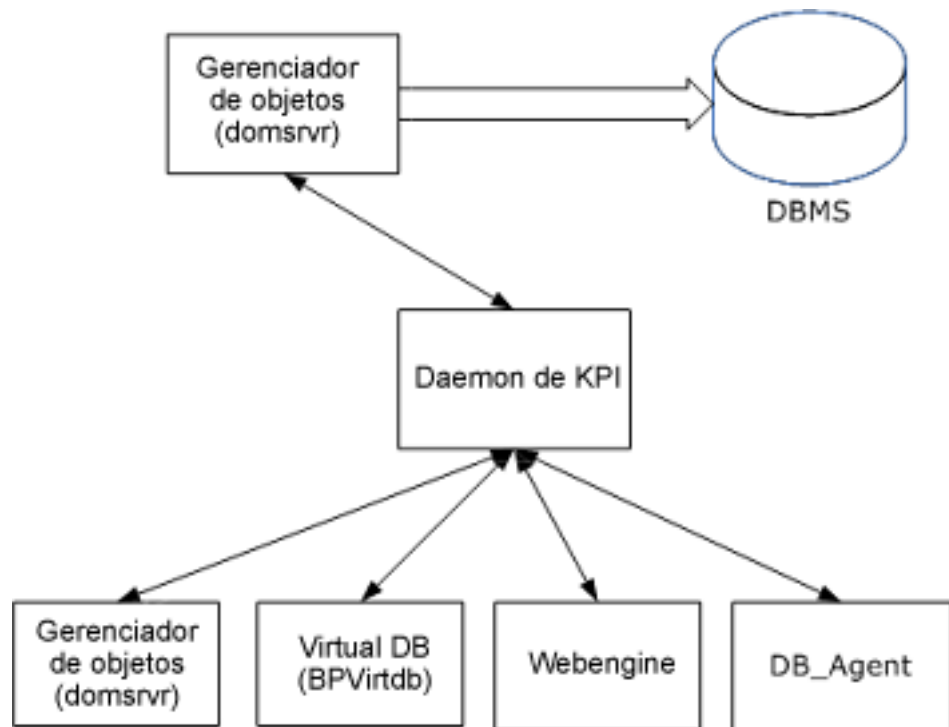
Os KPIs do sistema permitem a coleta de dados de métrica relacionados à operação dos processos do CA SDM.

Os seguintes tipos de processos são suportados:

- **domsrvr**—O CA SDM Object Manager (processo do servidor). O Object Manager também armazena em cache diversos registros e tabelas para os clientes.
- **bpvirtdb** — O servidor de banco de dados BOP virtual habilita operações de vários Gerenciadores de objetos no ambiente do CA SDM. Todos os Gerenciadores de objetos sendo executados em servidores primários ou secundários se conectam ao banco de dados virtual que arbitra sobre o acesso aos agentes de bancos de dados. Por exemplo, ao recuperar um novo intervalo de números de referência de ticket, o banco de dados virtual garante que apenas um Gerenciador de objetos de cada vez acessa a tabela contendo os números de referência. O banco de dados virtual também permite o armazenamento em cache das informações do banco de dados para os Gerenciadores de objetos.
- **db_agents**—Agentes de banco de dados que realizam consultas SQL e tratam de outras interações entre o CA SDM e o sistema de gerenciamento de banco de dados (DBMS). Os Agentes do banco de dados aderem ao esquema do banco de dados CA SDM e traduz o código SQL para a forma solicitada pelo DBMS específico (por exemplo, Oracle).

- **webengine**—O componente do CA SDM que conecta os navegadores da web a um Gerenciador de objetos através do pdmweb cgi sendo executado no servidor web Microsoft IIS ou Apache Tomcat. Deve haver um mecanismo da web para o WSP no servidor principal para que o Designer de esquemas do WSP possa gravar arquivos de esquema. Os mecanismos da web são os clientes reais de um Gerenciador de objetos para os navegadores da web de cliente do usuário. Os mecanismos da web armazenam em cache os formulários da web .htmpl para os usuários conectados. É possível manipular o armazenamento em cache usando o utilitário pdm_webcache e visualizar as estatísticas de conexão do cliente usando o utilitário pdm_webstat.

Observação: Para obter mais informações sobre esses processos, consulte o *Guia de Implementação*.

O diagrama a seguir ilustra o fluxo de dados para os KPIs do sistema.

Cada KPI do sistema cria um dos seguintes tipos de métrica a seguir:

- Contagem
- Duração

Exemplos de KPI do sistema

- Esse exemplo cria uma conta das solicitações de mudança enviadas para o banco de dados virtual BOP:

  ```
  updateCt
  ```

- Esse exemplo relata quanto tempo as solicitações de atualizações, inserções e exclusões do banco de dados virtual BOP levam para ser concluídas:

  ```
  virtdbUpdateResponseDt
  ```

KPIs de consulta armazenadas

Com os KPIs de consulta armazenadas é possível gerar relatórios com base nas métricas de conta recuperadas do banco de dados CA SDM.

O CA SDM oferece um conjunto de consultas pré-definidas armazenadas. Muitas delas são úteis da maneira que se encontram. É possível ainda personalizá-las para atender suas necessidades ou usá-las como modelos para criar suas próprias consultas.

Todos os KPIs de consulta armazenadas possuem uma métrica do tipo Conta.

Observação: é possível usar as consultas armazenadas para criar campos de contadores para os gerenciadores de filas da interface da web ou métricas de KPI, ou ambos. Para usar uma consulta em uma definição de KPI, a consulta deve ser habilitada para uso no KPI. Para obter mais informações, consulte Configuração das consultas armazenadas (na página 377).

Exemplos de KPI de consulta armazenada

- Esse exemplo cria uma conta das requisições de mudança abertas no local do responsável:

  ```
  Mudanças em @cnt.location.name
  ```

- Esse exemplo cria uma conta das tarefas de fluxo de trabalho irá violar um SLA antes da meia noite do dia atual:

  ```
  Tarefas do fluxo de trabalho da ocorrência que violarão um SLA hoje
  ```

KPIs SQL

Os KPIs SQL oferecem mais flexibilidade do que os KPIs de consultas armazenadas. Com os KPIs SQL é possível gravar suas próprias consultas do banco de dados do CA SDM para produzir os seguintes tipos de métricas:

- Somar
- Contagem
- Máx
- Duração

Observação: o código SQL deve estar em conformidade com a sintaxe SQL92.

As seguintes considerações se aplicam a KPIs de SQL:

- Para visualizar o código SQL para essas consultas de exemplo, abra as definições de consulta da página de Lista de KPI.

  Observação: para obter instruções, consulte a *Ajuda online*.

- O símbolo @ não é suportado pelos KPIs SQL. Em vez disso, use a sintaxe como mostrada no exemplo a seguir e um alias do atributo:

  ```
  SELECT * FROM cr WHERE assignee_last_name = "Smith"
  ```

  Por exemplo, é possível usar um alias de atributo predefinido. A página Detalhes do alias do atributo é exibida da seguinte maneira:

  " Nome de objeto = cr

  " Nome de alias = assignee_last_name

  " Status = Active

  " Valor do status = assignee.last_name

Exemplos: KPI de consulta SQL

- O exemplo predefinido gera uma soma dos custos estimados de todas as tarefas do fluxo de trabalho da requisição de mudança pendentes:

  ```
  Soma da estimativa de custo das tarefas do fluxo de trabalho de mudança pendentes
  ```

- O exemplo predefinido cria uma conta das requisições de mudança ativas que foram fechadas e reabertas:

  ```
  Conta das requisições de mudança reabertas
  ```

Campos KPI

A seguinte tabela a seguir descreve os campos de KPI. As colunas sys. S.Q. e SQL indicam os tipos de KPI ao qual cada campo pertence (Sistema, Consulta armazenada ou SQL).

Observação: todos os campos são obrigatórios a menos que sejam especificados como opcionais.

Campo	Sys.	S.Q.	SQL	Descrição
Nome do KPI	v	v	v	Identifica o nome de exibição do KPI. Não editável.
Tipo	v	v	v	O KPI define o registro como um KPI do sistema, de Consulta armazenada ou SQL. Não editável.
Manter versão existente	v	v	v	Especifica que a versão atual do registro de KPI será mantida se o registro for atualizado. Editável quando a definição @NX_ALWAYS_KEEP_KPI_VERSIONS no NX.env estiver configurada como Não.
Versão	v	v	v	Identifica o número da versão do registro de KPI. O número de versão é aumentado automaticamente sempre que o registro é atualizado. Não editável.
Status do registro	v	v	v	Especifica se o KPI está ativo (reunindo dados) ou inativo (não reunindo dados). Editável apenas ao usar o recurso "Editar na lista" na página Lista de KPIs.
Tipo de métrica	v	v	v	Especifica o tipo de cálculo que o KPI executará: ■ Os KPIs de consultas armazenadas sempre são Conta. ■ Os KPIs do sistema podem ser Conta ou Duração. ■ Os KPIs SQL podem ser Conta, Soma, Máx ou Duração. Editável apenas para o KPI do tipo SQL...
AtualizarTempo	v	v	v	Especifica o intervalo de tempo para recuperar as métricas de KPI do banco de dados. O valor é editável. O tempo de atualização é especificado no formato HH:MM:SS.

Campo	Sys.	S.Q.	SQL	Descrição
Tipo Tipo	v			As métricas do sistema PID (na página 863) podem ser produzidas a partir dos seguintes processos do CA SDM: ■ **domsrvr**—Gerenciador do objeto ■ **bpvirtdb**—Servidor de banco de dados BOP virtual. ■ **db_agents**—Agentes do banco de dados ■ **webengine**: o cliente web do CA SDM
Nome Nome	v			O nome interno do KPI do sistema Não editável.
Contexto do usuário		v	v	(Opcional) Especifica a ID do usuário de um contato do CA SDM. Atribuições de funções e inquilinos do contato são usadas para determinar a partição de dados para as métricas produzidas pelo KPI. O valor é editável.
Consulta Consulta		v		O nome da consulta armazenada chamada por esse KPI. O valor é editável.
Consulta Consulta			v	O código SQL para a consulta. O valor é editável.
Descrição	v	v	v	(Opcional) Fornece uma descrição detalhada do KPI. O valor é editável.

Recuperar dados de ticket

Para permitir a geração de relatório sobre o tempo em que os tickets permanecem nos vários estados de processamento, você pode configurar o daemon de KPI para recuperar dados do ticket do CA SDM sempre que um ticket for aberto ou fechado, e sempre que um dos valores dos campos a seguir for alterado:

- Ativo
- Responsável
- Área ou categoria
- Grupo
- Impacto
- Organização
- Prioridade

- Motivo raiz
- Status
- Tipo de serviço

Para ativar a recuperação de ticket, instale a opção Tabela de dados de ticket de KPI disponível na pasta KPI do Gerenciador de opções.

O conjunto de dados de tickets novos e atualizados é ativado. Os dados do ticket são gravados na tabela de banco de dados usp_kpi_ticket_data e ficam disponíveis para gerar relatórios com base na web.

Observação: para obter instruções, consulte a *Ajuda online*.

As seguintes considerações se aplicam à recuperação de ticket:

- O daemon do KPI pode levar até 30 minutos para preencher as informações do ticket para a tabela usp_kpi_ticket_data.
- O campo support_lev permite rastrear o processamento de Tipo de serviço quando a opção classic_sla_processing está instalada. A opção classic_sla_processing permite o processamento do Tipo de serviço do CA SDM versão 6.0 e anterior.
- Habilitar esse recurso pode reduzir o desempenho do CA SDM.

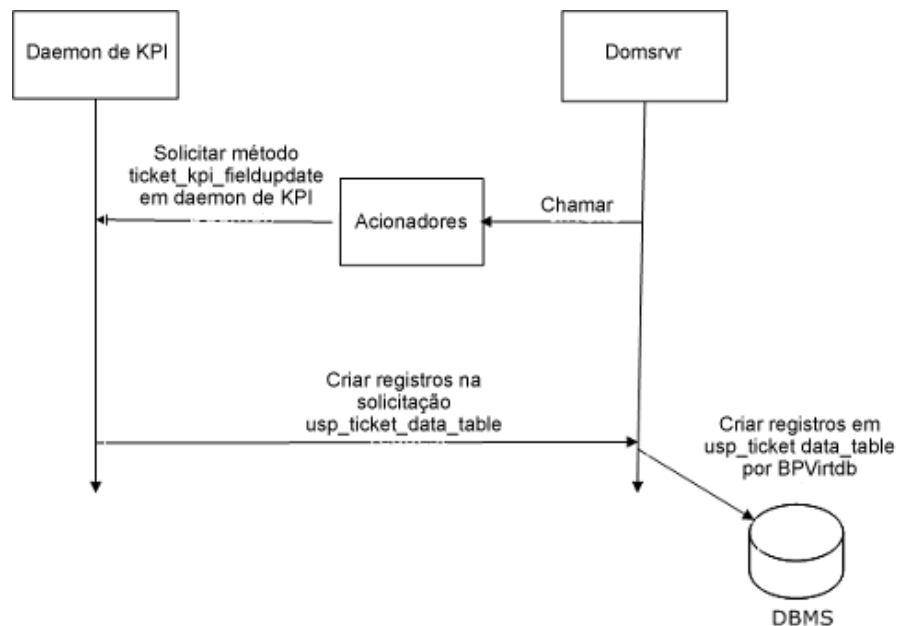
Mais informações:

Arquivo NX.env (na página 872)

Fluxo de dados do ticket de KPI

O recurso da Tabela de dados de ticket de KPI opera em um mecanismo de gatilho. Quando a opção kpi_ticket_data_table está instalada, o daemon do KPI começa a monitorar os objetos do ticket do CA SDM para acompanhar os seguintes eventos:

- Abertura de um novo ticket
- Verificação das mudanças para um ou mais campos monitorados
- Fechamento de ticket

Quando um desses eventos ocorre, o gatilho POST_CI é disparado. O gatilho envia uma BPMessage com a lista de atributos do gatilho para o daemon do KPI e adiciona os dados retornados na tabela usp_kpi_ticket_data, como ilustrado no diagrama de fluxo de dados a seguir.

Tipos de registro da tabela de dados de ticket do KPI

Há cinco tipos de operação na tabela usp_kpi_ticket_data:

- INIT (0)
- NO_INIT_REC (1)
- REOPEN (2)
- UPDATE (3)
- CLOSE (4)

O valor do tipo (valor inteiro exibido entre parênteses) é armazenado no campo de operação. O end_time do registro anterior é armazenado no campo prev_time. O campo ktd_duration armazena a duração, que é calculada com base no valor de end_time menos prev_time. O registro anterior é definido de acordo com as seguintes regras:

1. O registro INIT indica que um ticket foi criado.
2. Um registro UPDATE é criado para cada atualização em um ticket. Ele obtém prev_time de um registro UPDATE anterior para o mesmo campo de ticket caso já exista um registro UPDATE anterior. Caso contrário, ele obtém o prev_time do registro INIT, NO_INIT_REC ou REOPEN, dependendo de qual registro possui o valor mais próximo ao horário no registro UPDATE.
3. O registro CLOSE é o mesmo do UPDATE.
4. Se um ticket é reaberto, um registro REOPEN único é criado para mostrar o valor do campo Ativo. O registro REOPEN obtém o prev_time a partir de um registro CLOSE anterior para o mesmo campo Atividade.
5. Se um ticket foi criado antes da ativação da opção Gerenciador de opções, ele pode possuir registros para atualizações, mas sem um registro INIT. Nesse caso, o programa cria um registro NO_INIT_REC e obtém o prev_time a partir do primeiro registro não INIT encontrado.

Observação: para obter a documentação completa dos campos da tabela, consulte o *Guia de Referência Técnica*.

Solução de problemas

Você pode diagnosticar possíveis problemas com o uso de KPIs.

Verifique se o daemon do KPI está sendo executado.

Para verificar se o daemon do KPI está sendo executado, execute o utilitário de linha de comando pdm_status da seguinte maneira:

```
pdm_status
```

Examine a saída para:

```
KPI Daemon myserver  Running  myserver 3568  Wed Feb 06 07:23:53
```

Arquivo NX.env

Revise o arquivo $NX_ROOT/NX.env para verificar se as opções de KPI básicas foram definidas corretamente.

Caso tenha instalado a opção Tabela de dados de ticket de KPI, o arquivo NX.env inclui o seguinte:

```
####################################################################
# NX_KPI_TICKET_DATA_TABLE
# Enable the collection of changed fields from ticket objects
# (like Requests, Issues and Change Orders) to write record entries
# into the usp_kpi_ticket_data table.
####################################################################
@NX_KPI_TICKET_DATA_TABLE=Yes

####################################################################
# NX_KPI_FUZZ_TIME
# Specifies a tolerable delay for each KPI within which kpi_daemon
# sends a request to retreive KPI data when this kPI's refresh time
# is timeout
####################################################################
@NX_KPI_FUZZ_TIME=20
```

Observação: o valor padrão de @NX_KPI_FUZZ_TIME é 20 segundos. É possível modificar esse valor no intervalo de 0 a 40 segundos. Caso a variável seja definida com um valor superior a 40, o valor utilizado será 40 segundos.

```
####################################################################
# NX_ALWAYS_KEEP_KPI_VERSIONS
# The keep_version attribute in Kpi table is displayed on the KPI
# Detail Edit form as a checkbox. The NX_ALWAYS_KEEP_KPI_VERSIONS
# option specifies that checkbox is read-only and is always checked.
####################################################################
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

Ative o rastreamento do daemon do KPI

Use o utilitário pdm_logstat para ativar o log de rastreamento para monitorar a atividade do daemon do KPI.

Para ativar o rastreamento do daemon de KPI, execute o seguinte comando:

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

Para desativar o rastreamento do daemon de KPI, execute o seguinte comando:

```
pdm_logstat -f cache_table_mgr.c
```

Examine o arquivo stdlog.0 em busca de entradas pertencentes à atividade do daemon do KPI.

O exemplo a seguir mostra as conexões normais do daemon do KPI com o computador host e com o domsrvr:

```
02/06 05:42:14.58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c  117 KPIDaemon ready for
action!
02/06 05:42:14.80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Connecting client
kpi_daemon:garbo-2k3-bb
02/06 05:42:14.81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI daemon connected with domsrvr
```

O exemplo a seguir indica um erro em um KPI chamado webSessionCT:

```
01/16 13:24:46.74 jed web:local 2152 ERROR sys_kpi.c 96 Invalid KPI metric type: 1382180215 (KPI
name:webSessionCT)
```

Os exemplos a seguir mostram a atividade do daemon do KPI:

```
02/06 07:23:50.47 garbo-2k3-bb  kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created
Kpi_Obj (KPI dob record_id:9003) (KPI type:2)
02/06 07:23:50.53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c  427 Cache Table manager created
Kpi_Obj (KPI dob record_id:9103) (KPI type:1)
```

Observação: Para obter informações sobre os tipos de KPI, consulte Tipos de registro da tabela de dados de ticket do KPI (na página 870).

Relatórios ad hoc

Relatórios ad hoc são desenvolvidos no InfoView com o uso do Web Intelligence. Você pode criar relatórios ad hoc.

Observação: para obter informações sobre geração de relatório ad hoc, consulte a documentação do BusinessObjects Enterprise. Para acessar a documentação, clique no ícone de ajuda no InfoView.

Interface do Web Intelligence

No InfoView, o Web Intelligence fornece uma ferramenta para geração de relatórios personalizados destinada a usuários que pretendem criar relatórios básicos com facilidade sem criar consultas. O Web Intelligence usa modelos predefinidos de relatório e modelos que gerenciam conexões de dados, consultas e relacionamentos de dados. Assim, você só precisa arrastar e soltar os campos de dados sobre um modelo para criar relatórios tabulares ou de matriz. Você pode usar todos os recursos do InfoView descritos no *Guia do Usuário do InfoView*.

Para criar relatórios, um documento do Web Intelligence faz referência a um objeto do BusinessObjects chamado de universo. Você cria os novos relatórios nos universos do BusinessObjects. O CA Business Intelligence fornece o universo do CA SDM com o produto.

Como funciona a geração de relatório ad hoc

A geração de relatório ad hoc funciona da seguinte maneira:

1. Inicie o relatório ad-hoc ao selecionar primeiro o universo do CA SDM no InfoView.
2. O universo mapeia para o banco de dados do CA SDM que contém informações de negócios organização. Quando você se conecta a um universo, o Web Intelligence inicia automaticamente o editor de documentos selecionado na página Document Preferences do Web Intelligence no InfoView.

   Observação: para obter informações sobre como definir preferências, consulte o *Guia do Usuário do InfoView*.
3. Usando o universo, é possível criar consultas para recuperar dados a serem usados em um relatório a partir dos objetos agrupados em pastas chamadas classes. Cada classe também pode conter uma ou mais subclasses. As subclasses contêm objetos que, por sua vez, são uma subcategoria dos objetos do nível superior da classe. As classes e os objetos são apresentados em uma estrutura de árvore (hierarquia) na guia Data.

   Observação: para obter instruções sobre como criar consultas para documentos do Web Intelligence, consulte a documentação do BusinessObjects Enterprise.
4. Após criar sua consulta adicionando os objetos necessários na seção Result Objects e definir as propriedades de filtro da consulta, você está pronto para executar a consulta. Quando você executa uma consulta, o universo pede que o banco de dados recupere os dados correspondentes às necessidades de cada objeto na consulta. Para executar uma consulta, clique em Executar consulta na barra de ferramentas.

   Importante: Ao selecionar objetos para sua consulta, sempre escolha objetos, medidas e filtros somente de uma classe base do universo e suas subclasses. Caso inclua objetos, medidas e filtros a partir de diversas classes básicas do universo em uma consulta, é possível receber resultados inesperados ou um desempenho ruim.

Exemplo de Relatórios ad hoc

Você pode trabalhar com o Web Intelligence e exemplos de consulta para criar relatórios ad hoc usando o universo CA SDM padrão. Quando criar um relatório, assegure-se de salvá-lo em intervalos regulares. Se a sessão de conexão do Web Intelligence expirar, você perderá as modificações do relatório.

Observação: para obter informações sobre como alterar o valor do tempo limite da sessão, consulte o *Guia de Implementação*.

Exemplo: Exibir todas as solicitações abertas de prioridade 1 e 2 para todos os usuários

Nesse exemplo, você irá especificar valores de prompt que irão reunir dados adicionais antes de gerar o relatório.

Exemplo: Exibir todas as solicitações abertas de prioridade 1 e 2 para todos os usuários

1. Clique em Novo, Web Intelligence Document na barra de menus.

   A página New Web Intelligence Document aparece.

2. Selecione o universo do CA SDM na coluna Universe.

   O documento do Web Intelligence aparece com as informações de universo no painel esquerdo.

   Observação: para melhor navegação, feche a pasta Tipo de serviço vinculado no painel esquerdo.

3. Localize e em seguida expanda as pastas Solicitação, Detalhe de solicitação na seção esquerda. Use a barra de rolagem para localizar as pastas.

4. Seleciona cada um dos seguintes objetos, em seguida os arrasta e solta da seção esquerda para a seção superior direita sob Results Objects.

   - Resumo
   - Símbolo de prioridade
   - Nome do combo do cliente

5. Selecione os seguintes objetos e arraste solte-os na seção inferior direita em Query Filters. Feche a pasta Detalhes da solicitação quando terminar.

   - Símbolo de status
   - Símbolo de prioridade

6. Expanda a pasta Filtros de solicitação, então arraste e solte o filtro Customer Combo Name with Userid para a seção inferior direita em Query Filters.
7. Na seção Query Filters, clique na seta na lista no filtro Símbolo de status e selecione o operador Equal to.
8. Selecione o(s) valore(s) na lista do menu Operand Type.

   A caixa de diálogo Lista de valores aparece.
9. Na lista Símbolo de status, selecione Abrir e clique na seta verde.

   O valor é exibido no campo Valor(es) selecionado(s).
10. Clique em OK.
11. Na seção Query Filters, clique no menu suspenso na lista no filtro Símbolo de prioridade e selecione o operador In List.
12. Na lista Símbolo de prioridade, selecione simultaneamente 1 e 2 e clique na seta verde.

    Os valores 1 e 2 são exibidos no campo Value(s) Selected.
13. Clique em OK.
14. Clique em Executar consulta na barra de ferramentas para gerar o relatório.

    Observação: uma vez o filtro rápido Customer Combo Name with Userid utiliza a função Prompt, a caixa de diálogo Prompt é exibida. Esta caixa de diálogo permite reunir dados adicionais antes que o relatório seja gerado.
15. Na janela Prompts, selecione a opção TODOS e clique no botão com a seta verde.

    Todos os nomes de usuário aparecem na lista Select Customer.
16. Clique em Executar consulta para gerar o relatório.

    O relatório aparece em uma nova janela.
17. Clique duas vezes no título do relatório e digite Solicitações abertas de prioridade 1 e 2 para todos os usuários na caixa de texto. Você pode alterar o tamanho de fonte para 16 ou outros tamanhos.
18. Para alterar outros aspectos do relatório, clique na guia Propriedades.
19. Para subagrupar os dados pelo Sobrenome do cliente, clique com o botão direito do mouse em qualquer célula na coluna Sobrenome do cliente e selecione Set as Section.
20. Clique em Salvar e especifique um local usando a opção Salvar como.

Exemplo: exibir todas as solicitações abertas que não incluem um status de trabalho em andamento

Nesse exemplo, você especificará que a função de geração de relatório Contagem deve retornar o número total de solicitações em aberto.

Exemplo: exibir todas as solicitações abertas que não possuem um status de trabalho em andamento

1. Clique em Novo, Web Intelligence Document na barra de menus.

   A página New Web Intelligence Document aparece.

2. Selecione o universo do CA SDM na coluna Universe.

   O documento do Web Intelligence aparece com as informações de universo no painel esquerdo.

   Observação: para melhor navegação, feche a pasta Tipo de serviço vinculado no painel esquerdo.

3. Localize e em seguida expanda as pastas Solicitação, Detalhe de solicitação na seção esquerda. (Use a barra de rolagem para navegar pelas pastas.)

4. Seleciona cada um dos seguintes objetos, em seguida os arrasta e solta da seção esquerda para a seção superior direita sob Results Objects.

   - Símbolo de status
   - No. de ref.
   - Resumo

5. Selecione o objeto do Símbolo de status, então arraste e solte-o na seção inferior direito em Query Filters. Feche a pasta Detalhes da solicitação.

6. Expanda a pasta Filtros de solicitação, então arraste e solte o filtro Ativo para a seção inferior direito em Query Filters.

7. Na seção Query Filters, clique na seta na lista no objeto Símbolo de status e selecione o operador Not Equal to.

8. Selecione Trabalho em andamento no menu Operand Type.

9. Clique em Editar relatório na barra de ferramentas principal.

   O Report Viewer abre.

10. No relatório, selecione a coluna Nº de ref.[Essa ação ativa o comando Insert Sum na barra de ferramentas Relatar.

11. Clique no comando Insert Sum e selecione Conta no menu.

12. No relatório, clique com o botão direito do mouse na célula =[Status Symbol] e selecione Set as Section no menu de contexto.
13. Clique em Refresh Data na barra de ferramentas principal para executar o relatório.
14. Clique em Salvar.

    O relatório exibe o número total (conta) de solicitações que *não* possuem o status Trabalho em andamento.

Exemplo: Exibir todas as solicitações fechadas nos últimos 30 dias por usuários cujos sobrenomes começam com "C"

Nesse exemplo, serão especificados valores de prompt para Data de fechamento e Sobrenome do cliente que irão retornar todas as solicitações fechadas com base nesses valores.

Exemplo: Exibir todas as solicitações fechadas nos últimos 30 dias por usuários cujos sobrenomes começam com "C"

1. Clique em Novo, Web Intelligence Document na barra de menus.

   A página New Web Intelligence Document aparece.

2. Selecione o universo do CA SDM na coluna Universe.

   O documento do Web Intelligence aparece com as informações de universo no painel esquerdo.

   Observação: para melhor navegação, feche a pasta Tipo de serviço vinculado no painel esquerdo.

3. Localize e expanda as pastas Solicitação, Detalhes da solicitação na seção esquerda. Use a barra de rolagem para navegar pelas pastas.
4. Seleciona cada um dos seguintes objetos, em seguida os arrasta e solta da seção esquerda para a seção superior direita sob Results Objects.
   - No. de ref.
   - Data de fechamento
   - Sobrenome do cliente
   - Resumo

5. Selecione cada um dos seguintes objetos e arraste-os para a seção inferior direito em Query Filters.
   - Símbolo de status
   - Data de fechamento
   - Sobrenome do cliente
6. Clique na seta na lista no filtro Símbolo de status e selecione Valor(es) a partir da lista do menu Operand Type.

   A caixa de diálogo Lista de valores aparece.
7. Selecione os seguintes valores na lista de Símbolo de status:
   - Fechado
   - Fechado-Não resolvido
   - Solicitação fechada
   - Problema fechado
   - Problema corrigido
   - Resolvido
8. Clique na seta verde.

   Os valores são exibidos no campo Value(s) Selected.
9. Clique em OK.
10. Na seção Query Filters, clique na seta na lista no objeto Data de fechamento e selecione o operador Between.
11. Clique na seta na lista e selecione os menus Prompt from the first and second Operand Type.
12. Clique na seta na lista no objeto Sobrenome do cliente e selecione o operador Matches pattern.
13. Clique na seta na lista e selecione o menu Prompt from the Operand Type.
14. Clique no ícone Prompt Properties que aparece próximo à seta na lista.

    A caixa de diálogo Prompt é exibida.
15. No campo de texto Prompt, insira um padrão para Sobrenome do cliente.
16. Clique em OK.

17. Clique em Executar consulta na barra de ferramentas para gerar o relatório.

    Observação: uma vez os objetos Sobrenome do cliente e Data de fechamento usam a função Prompt, a caixa de diálogo Prompt é exibida. Esta caixa de diálogo permite reunir dados adicionais antes que o relatório seja gerado.

18. Na janela Prompts, selecione ou digite os valores de prompt para cada prompt da seguinte maneira:

    - Insira a Data de fechamento (Início): Especifique uma data que seja 30 dias antes da data atual.
    - Insira a Data de Fechamento (Término): Especifique a data atual.
    - Insira um padrão para o Sobrenome do cliente: especifique C%.

19. Clique em Executar consulta para gerar o relatório.

    O relatório aparece em uma nova janela.

20. Clique duas vezes sobre o título do relatório e digite Exibir todas as solicitações fechadas nos últimos 30 dias para usuários cujos sobrenomes comecem com "C" na caixa de texto. Você pode alterar o tamanho de fonte para 16 ou outros tamanhos.

21. Para alterar outros aspectos do relatório, clique na guia Propriedades.

22. Clique em Salvar e especifique um local usando a opção Salvar como.

Relatórios do painel

É possível usar os relatórios do console para monitorar as operações diárias para todos os tipos de tickets do CA SDM (solicitação/incidente/problema, requisição de mudança ou ocorrência) no Gerenciamento de conhecimento, Support Automation e CMDB no BusinessObjects InfoView. Cada relatório contém dados analíticos sobre aqueles com os melhores desempenhos no trabalho com tickets ativos, para que você possa monitorar seu progresso.

Com o relatório de painel é possível:

- Exibir o resumo e informações detalhadas sobre os tickets ativos por prioridade, analista, categoria ou grupo.
- Descobrir quantos tickets foram resolvidos em um espaço de tempo determinado e muito mais.
- Editar, imprimir, acompanhar e salvar os relatórios em outros formatos, como .xls e .pdf.

É possível trabalhar com relatórios individuais de painel predefinidos ou usar o painel corporativo para exibir todas as operações diárias do CA SDM em uma única exibição. O painel corporativo compartilha informações vitais sobre as operações diárias para todos os tipos de ticket (solicitação/incidente/problema, requisição de mudança ou solicitação) por prioridade, analista, categoria ou grupo.

Observação: quando trabalhar com o sistema de geração de relatórios do console, é possível usar os recursos do InfoView que são descritos na seção Trabalhando com console e analítica do *Guia do Usuário do BusinessObjects InfoView*. Para acessar o Guia do Usuário, clique no ícone de ajuda no InfoView.

Exibir Painéis e Relatórios no InfoView

A conta de administrador pode fazer logon e exibir os relatórios no BusinessObjects InfoView. As pastas e relatórios exibidos que os usuários vêem no InfoView dependem da conta com a qual efetuam logon e dos direitos concedidos para a conta.

Para verificar os painéis relatórios no InfoView

1. Efetue logon no CA SDM.
2. Na guia Relatórios clique no botão InfoView.

   O InfoView aparece em seu navegador web.
3. Na barra de ferramentas do InfoView, selecione Lista de documentos.

   Pastas e objetos aparecem na área de navegação.
4. Selecione Public Folders, CA Reports, CA SDM Dashboards.

   As seguintes pastas são exibidas: Requisição de mudança, Incidente, Ocorrência, Problema, Solicitação, Configuração e Conhecimento.
5. Selecione o relatório apropriado.

   O relatório é exibido no painel direito.
6. Clique duas vezes no título para exibir um relatório.

   O relatório é aberto para exibição.

Gravar relatórios do CA Business Intelligence

É possível gravar relatórios do CA Business Intelligence para o CA SDM.

Mais informações:

Driver ODBC do CA SDM (na página 882)
Escrever SQL para relatórios BusinessObjects (na página 883)
Funções do PDM (na página 884)
Alias de atributo (na página 887)
SQL interativo pdm_isql (na página 887)

Driver ODBC do CA SDM

Os aplicativos de relatório do Business Objects (Crystal Reports e Web Intelligence) acessam dados usando um driver ODBC que estabelece conexão direta com o mecanismo de objeto do CA SDM com o nome domsrvr.

Essa conexão oferece inúmeros benefícios:

- As instruções SELECT usadas pelos relatórios do BusinessObjects fazem referência a objetos e atributos usando seus nomes de CA SDM (em outras palavras, seus nomes Majic). Por exemplo, uma instrução SELECT para um relatório em contatos deve ser escrita:
  ```
  SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'
  ```
- O driver OBDC do CA SDM mapeia atributos como combo_name e objetos como cnt aos seus nomes de DBMS correspondentes.
- Toda a segurança do CA SDM, inclusive partição de dados e restrições de locação, é automaticamente aplicada aos relatórios. Todas as conexões entre BusinessObjects e CA SDM são associadas a um contato do CA SDM, e o ODBC do CA SDM edita instruções SELECT de entrada para aplicar as restrições de segurança associadas à função de relatório do usuário final. O BusinessObjects não é conectado diretamente ao banco de dados.
- O recurso Alias do atributo do CA SDM "achata" ou desnormaliza o banco de dados do CA SDM. Os aliases de atributo são atributos adicionais nos objetos do CA SDM que permitem uma consulta a atributos de referência em tabelas unidas sem uma junção específica, permitindo que a tabela base seja usada como se fosse um modo de exibição de relatório.

- O driver ODBC do CA SDM oferece suporte a literais de dados em consultas e automaticamente converte valores no formato de data interno do CA SDM em uma data DBMS padrão.

Importante: O driver ODBC do CA SDM é suportado apenas para relatório de BusinessObjects (Crystal e Web Intelligence). O CA SDM não fornece um cliente ODBC autônomo e não recomenda o uso de um driver ODBC com aplicativos que não sejam o BusinessObjects.

Escrever SQL para relatórios BusinessObjects

Todas as instruções SQL usadas pelos relatórios do BusinessObjects são processadas pelo driver ODBC do CA SDM. O driver ODBC oferece suporte a instruções SQL 92 SELECT com as seguintes alterações ou extensões:

- Os nomes de objetos do CA SDM são usados no lugar de nomes de tabela do DBMS, e os nomes de atributo do CA SDM são usados no lugar de nomes de coluna do DBMS.
- Um nome de alias de atributo do CA SDM pode ser usado em qualquer lugar da consulta onde um nome de coluna é válido. O driver do ODBC substitui a referência de alias de atributo por uma ou mais uniões.

  Observação: para obter mais informações, consulte Aliases de atributo (na página 887).
- Atributos DERIVED do CA SDM (como combo_name) podem ser usados apenas na lista de seleção. Eles não são suportados em nenhuma outra parte da consulta, incluindo a cláusula WHERE.

  Observação: muitos objetos de nome de combinação com ID de usuário são fornecidos no universo, como o nome de combinação de cliente com objeto de ID de usuário utilizado como filtro no exemplo de relatório ad hoc fornecido no *Guia de Administração*. Esses objetos permitem que o nome de combinação seja usado como solicitações de filtro em consultas ad hoc com Web Intelligence, para superar a limitação de incluir o nome de combinação na cláusula WHERE. Eles apresentam nome de combinação e a ID de usuário na solicitação de filtro, mas usam apenas as IDs de usuário selecionadas na consulta SQL resultante.
- As consultas podem conter literais de data em qualquer uma das formas:

  ```
  d'aaaa-mm-dd hh:mm:ss xm' (em que xm é am ou pm)
  ts'aaaa-mm-dd hh:mm:ss'
  ```

  Esses literais podem ser usados em qualquer lugar da consulta. O driver ODBC automaticamente os converte no formato de data interno do CA SDM (o número de segundos a partir da meia-noite de 1 de janeiro de 1970).

Funções do PDM

Para ajudar no trabalho com recursos e tipos de dados especializados do CA SDM, o driver ODBC estende SQL para oferecer suporte a um número de funções de consulta adicionais. Todas as funções suportadas por driver começam com a sequência de caracteres "Pdm", e são conhecidas como funções PDM, conforme descrito na seguinte tabela:

Funções do PDM	Descrição
PdmAddDays([date,] count)	Quando usada com um argumento, adiciona o número de dias ao seu argumento para a data de hoje e retorna o resultado. Quando usada com dois argumentos, adiciona o número de dias ao seu segundo argumento para o valor da coluna de data especificado em seu primeiro argumento e retorna o resultado. Essa função pode ser usada em qualquer lugar da consulta.
PdmAddMonths([date,] count)	Quando usada com um argumento, adiciona o número de meses ao seu argumento para a data de hoje e retorna o resultado. Quando usada com dois argumentos, adiciona o número de meses ao seu segundo argumento para o valor da coluna de data especificado em seu primeiro argumento e retorna o resultado. O formato de argumento único pode ser usado em qualquer lugar da consulta. O formato de dois argumentos pode ser usado apenas na lista de seleção.
PdmDay([data])	Quando usado sem argumentos, retorna o dia atual como um número inteiro. Quando usado com um argumento, retorna o dia associado com o valor da coluna data especificada em seu argumento. A forma sem argumentospode ser usada em qualquer local da consulta. A forma comum argumentopode ser usada somente na lista da seleções.
PdmDownTime(slaName, workshift, startDate, endDate)	Calcula o tempo de inatividade entre duas datas no turno de trabalho e no SLA especificados. Essa função pode ser usada somente na lista de seleções
PdmMonth([date])	Quando usada sem nenhum argumento, retorna o mês atual como um inteiro de 1 a 12. Quando usada com um argumento, retorna o mês associado ao valor da coluna de data especificado em seu argumento. A forma sem argumentospode ser usada em qualquer local da consulta. A forma comum argumentopode ser usada somente na lista da seleções.

Funções do PDM	**Descrição**
PdmMonthName([date])	Quando usado sem nenhum argumento, retorna o nome localizado do mês atual ("janeiro", "fevereiro" etc). Quando usada com um argumento, retorna o nome localizado do valor da coluna de data especificado em seu argumento. A forma sem argumentospode ser usada em qualquer local da consulta. A forma comum argumentopode ser usada somente na lista da seleções.
PdmDay([data])	Quando usado sem argumentos, retorna o dia atual como um número inteiro. Quando usado com um argumento, retorna o dia associado com o valor da coluna data especificada em seu argumento. A forma sem argumentospode ser usada em qualquer local da consulta. A forma comum argumentopode ser usada somente na lista da seleções.
PdmSeconds(date)	Retorna o valor da coluna de data especificado em seu argumento em sua forma bruta como o número de segundos a partir de 1 de janeiro de 1970. Essa função pode ser usada somente na lista de seleções Esse argumento é obrigatório.
PdmString(column)	Retorna a sequência de caracteres equivalente do valor da coluna especificado em seu argumento. Essa função pode ser usada com UUID, data ou colunas de sequência de caracteres. Pode ser usada somente na lista de seleções.

Funções do PDM	Descrição
PdmToday()	PdmToday() [timeAdj [, day [, month [, year]]]]) Avalia para a data de hoje (em segundos de 01/01/70), ajustado de acordo com os argumentos: timeAdj: -1—ajuste a hora para o começo do dia (0:00:00); +1—ajuste a hora para o fim do dia (23:59:59) dia: negativo—ajuste a data pelo número de dias especificado positivo—define o dia para o valor absoluto especificado (ou último dia do mês, o que for menor) mês: negativo—ajuste a data pelo número de meses especificado positivo—define o mês para o valor absoluto especificado (ou para dezembro (12), o que for menor) ano: negativo—ajuste a data pelo número de anos especificado positivo—define o ano para o valor absoluto especificado Os ajustes são aplicados na ordem ano, mês, dia. Um zero ou argumento omitido é ignorado.
PdmYear([date])	Quando usada sem nenhum argumento, retorna o ano atual como um inteiro de quatro dígitos. Quando usada com um argumento, retorna o ano associado ao valor da coluna de data especificado em seu argumento. A forma sem argumentospode ser usada em qualquer local da consulta. A forma comum argumentopode ser usada somente na lista da seleções.

Alias de atributo

Os aliases de atributo são atributos adicionais nos objetos do CA SDM que fazem referência a dados de tabelas unidas com o uso da sintaxe de união com pontos Majic (em que a sintaxe srelname.attrname é uma referência ao atributo attrname na tabela mencionado pelo srelname de chave estrangeira. Diversos aliases de atributo predefinidos são fornecidos com o CA SDM Release 12.7, com nomes que geralmente são iguais aos das uniões Majic correspondentes, com sublinhado substituindo o ponto que indica a união. Por exemplo, a seguinte instrução SELECT pode ser usada por um relatório que lista informações sobre os responsáveis da solicitação:

```
SELECT ref_num, assignee_combo_name, assignee_organization_name
   FROM cr WHERE customer_last_name LIKE 'smith%'
```

O driver ODBC do CA SDM cria uniões automaticamente de acordo com a necessidade para acessar as tabelas mencionadas pelos aliases de atributo. Um usuário na função de administrador do CA SDM pode facilmente adicionar novos aliases de atributo online, fornecendo uma coluna por vez para estender a exibição correspondente a um objeto.

Para acessar a tabela Alias do atributo, selecione a guia Administração e navegue até CA SDM, Códigos, Alias do atributo.

SQL interativo pdm_isql

Um utilitário de linha de comando, pdm_isql, é fornecido com CA SDM para permitir a entrada interativa de instruções SQL SELECT. As instruções SELECT inseridas em pdm_isql são enviadas ao driver ODBC CA SDM, permitindo que você teste as instruções SQL SELECT fora do BusinessObjects.

Para usar pdm_isql

1. Verifique se $NX_ROOT/bin está no caminho.
2. Digite o comando:

   pdm_isql

3. No prompt de pdm_isql, digite o comando a seguir:

   connect *username*password@casd_hostname*

   (em que *username* e *password* são credenciais de logon do CA SDM válidas, e hostname é o nome de host de um servidor CA SDM com um mecanismo web.)

4. Especifique instruções SQL select seguidas por um ponto e vírgula.

Capítulo 18: Gerando relatórios no CA SDM

Esta seção contém os seguintes tópicos:

Gerar relatórios (na página 889)
Exibições de banco de dados (na página 889)
Configuração de método de relatório (na página 893)
Formatação de relatórios (na página 894)
Modificação da ordem de classificação de colunas (na página 895)
Relatórios de detalhes e de resumo (na página 895)
Relatórios de análise (na página 895)

Gerar relatórios

O CA SDM fornece várias opções e recursos de geração de relatório integrados, incluindo:

- Imprimir formulários para ativos, ocorrências, incidentes, problemas, requisições de mudança individuais e muito mais.
- Gerar relatórios de resumo ou de detalhes para listas de requisições de mudança, ocorrências, incidentes, problemas, solicitações, itens de configuração.
- Gerar relatórios de análise.

Observação: para obter informações sobre como usar relatórios do CA SDM, consulte Gerando relatórios na *Ajuda online*. Além de usar os recursos de geração de relatório internos do CA SDM, você pode criar e gerar relatórios personalizados com base nas tabelas e exibições do banco de dados do CA SDM. Para obter mais informações sobre relatórios personalizados, consulte o *Guia de Implementação*.

Exibições de banco de dados

O banco de dados do CA SDM é um repositório de dados inseridos e usados para operar seu service desk. O CA SDM fornece várias exibições de banco de dados e permite criar relatórios personalizados do banco de dados.

Essas exibições são de dois tipos:

- Básico
- Avançado

Mais informações:

Exibir descrições de campo (na página 1083)

Tipo de exibição básico

As exibições básicas baseiam-se nas tabelas do CA SDM. Essas exibições mostram dados quando a implementação utiliza Solicitações, Incidentes, Problemas, Requisições de mudança, Ocorrências, Ativos ou Contatos / Grupos.

Ao usar as exibições básicas, você pode projetar e produzir vários relatórios, incluindo:

- Listas detalhadas e resumidas de solicitações abertas com prioridade 1 classificadas por área de solicitação.
- Listas detalhadas e resumidas de requisições de mudança atribuídas ao grupo de nível 1 que estejam abertas durante mais de 24 horas, classificadas por prioridade.
- Contagens de ocorrências abertas durante mais de um número especificado de dias, classificadas por prioridade, grupo atribuído, ou prioridade e grupo atribuído.

As seguintes exibições básicas são fornecidas:

Nome da exibição	Descrição
View_Contact_Full	Todos os contatos, incluindo seu tipo de contato, local, organizações e tipos de serviço
View_Contact_to_Environment	Todo os contatos e seu ambiente (ativos)
View_Group	Todos os grupos definidos no banco de dados
View_Group_To_Contact	Todo os contatos (incluindo gerentes) em suas atribuições a grupos

Nome da exibição	Descrição
View_Request	Todas as solicitações, incluindo seus tipos de serviço, gravidades, urgências, categorias, ativos, números de impacto, destinatários por nome, clientes por nome, grupos, status e prioridades
View_Act_Log	As informações de log das atividades de solicitação, incluindo tipo de atividade e nome do analista
View_Request_to_Act_Log	Todas as solicitações com seus logs de atividades (essa exibição une View_Request e View_Act_Log)
View_Request_to_Properties	As solicitações e suas propriedades (isso pode não incluir todas as solicitações, especialmente se nenhuma propriedade tiver sido atribuída a elas)
View_Change	Todas as requisições de mudança, incluindo seus status, prioridades, categorias, organizações, usuários finais afetados por nome, solicitantes por nome, destinatários por nome, grupos, tipos de serviço e números de impacto
View_Change_Act_Log	Informações do log de atividades da requisição de mudança
View_Change_to_Change_Act _Log	Todas as requisições de mudança com seus logs de atividades (essa exibição une View_Change e View_Change_Act_Log)
View_Change_to_Properties	As requisições de mudança e suas propriedades (isso pode não incluir todas as requisições de mudança, especialmente se nenhuma propriedade tiver sido atribuída a eles)
View_Change_to_Change_WF	As requisições mudança e suas tarefas de fluxo de trabalho (isso pode não incluir todas as requisições de mudança, especialmente se nenhuma tarefa de fluxo de trabalho tiver sido atribuída a elas)
View_Change_to_Assets	As requisições mudança e seus ativos (isso pode não incluir todas as requisições de mudança, especialmente se não tiverem nenhum ativo)
View_Change_to_Requests	As requisições mudança com informações básicas sobre solicitações vinculadas (essa exibição une as tabelas View_Change e Call_Request, o que pode não incluir todas as requisições de mudança — especialmente se nenhuma solicitação tiver sido vinculada a elas)

Nome da exibição	Descrição
View_Issue	Todas as ocorrências, incluindo seus status, prioridades, categorias, organizações, usuários finais afetados por nome, destinatários por nome, grupos, tipos de serviço e assim por diante
View_Issue_Act_Log	Informações do log de atividade da ocorrência
View_Issue_to_Issue_Act_Log	Todas as ocorrências com seus logs de atividades (essa exibição une View_Issue e View_Issue_Act_Log)
View_Issue_to_Properties	As ocorrências e suas propriedades (isso pode não incluir todas as ocorrências, especialmente se nenhuma propriedade tiver sido atribuída a elas)
View_Issue_to_Issue_WF	As requisições de mudança e suas tarefas de fluxo de trabalho (isso pode não incluir todas as requisições de mudança, especialmente se nenhuma tarefa de fluxo de trabalho tiver sido atribuída a elas)
View_Issue_to_Assets	As ocorrências e seus ativos (isso pode não incluir todas as ocorrências, especialmente se não tiverem nenhum ativo)

Exibições avançadas

As exibições avançadas baseiam-se na tabela audit_log do CA SDM.

Observação: Você deve instalar o audit_ins e /ou as opções de audit_upd no Gerenciador de opções e reinicializar o sistema antes de usar essas exibições.

Ao usar as exibições avançadas, você pode informar sobre a duração de um ticket (isto é, solicitação, requisição de mudança ou ocorrência) em um estado particular. Por exemplo, você pode gerar relatórios para:

- Mostrar a duração entre a abertura e a atribuição ao nível 2 de solicitações abertas desde 1º de janeiro de 2002
- Mostrar por quanto tempo ocorrências permaneceram com prioridade 3 antes de serem promovidas à prioridade 2 para ocorrências abertas desde 1º de janeiro de 2002

As seguintes exibições avançadas são fornecidas, as quais são exibições da tabela audit_log no banco de dados do CA SDM que consultam especificamente o status, a prioridade, o grupo ou os atributos de destinatário:

Nome da exibição	Descrição
View_Audit_Status	Todos os tickets classificados pelo tempo em cada status (não inclui tickets que não tenham status atribuídos)
View_Audit_Priority	Todos os tickets classificados por períodos de tempo em cada prioridade
View_Audit_Group	Todos os tickets classificados por períodos de tempo em cada atribuição (não inclui tickets que não tenham status atribuídos)
View_Audit_Assignee	Todos os tickets classificados por períodos de tempo em cada atribuição (não inclui tickets que não tenham destinatários atribuídos)

Importante: Você deve instalar opções de log de auditoria usando o Gerenciador de opções para exibir dados nas exibições avançadas. As descrições das opções de auditoria audit_ins e audit_upd na Ajuda online fornecem mais informações.

Mais informações:

Uso do Gerenciador de opções (na página 381)

Configuração de método de relatório

Os métodos de relatório permitem especificar para onde enviar os resultados de relatórios quando selecionar um relatório. Exemplos disso são relatórios resumidos e de detalhes disponíveis no menu Relatório e os relatórios disponíveis no menu Análise. Vários métodos de relatório predefinidos são fornecidos, e você pode modificá-los.

Observação: para obter informações sobre como definir métodos de relatório, consulte a *Ajuda online*.

Formatação de relatórios

Usando o arquivo dataent.fmt encontrado em $NX_ROOT/fig/cfg (UNIX) ou diretório_instalação\fig\cfg (Windows), você pode personalizar vários formatos de dados nos relatórios que imprimir. é possível ver e modificar esse arquivo usando qualquer editor de texto (usuários do Windows devem usar o WordPad para editar o arquivo).

As seguintes linhas no arquivo controlam alguns formatos de data e hora:

```
default_date = "long_date"
short_date = "M/D/YY// Digite a data como MM/DD/YY"
long_date = "MM/DD/YYYY// Digite a data como MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Digite uma hora no formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Digite uma hora no formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Digite uma hora no formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Digite uma hora no formato 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Digite uma data e hora no formato MM/DD/YY
hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Digite uma data e hora no formato MM/DD/YY
00:00:00-23:59:59"
```

Um exemplo de como é possível alterar essas linhas para dar suporte a datas e horas européias é mostrado a seguir:

```
default_date = "long_date"
short_date = "D/M/YY// Digite a data como DD/MM/YY"
long_date = "DD/MM/YYYY// Digite a data como DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Digite uma hora no formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Digite uma hora no formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Digite uma hora no formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Digite uma hora no formato 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Digite uma data e hora no formato MM/DD/YY
hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Digite uma data e hora no formato MM/DD/YY
00:00:00-23:59:59"
```

Observação: Se você estiver usando pdm_extract para exportar dados do banco de dados do CA SDM a outro sistema, e deseja extrair dados para usar o formato de data especificado no arquivo dataent.fmt, use o sinalizador -d quando chamar o pdm_extract.

Modificação da ordem de classificação de colunas

Os administradores podem modificar a ordem de classificações das colunas que são exibidas em relatórios usando o Pintor de tela da Web.

Os usuários podem classificar dados nas seguintes requisições:

- Crescente (A a Z, zero a 9, ou da primeira à última data)
- Decrescente (Z a A, 9 a zero ou da última à primeira data)

Observação: Para obter mais informações, consulte a *Ajuda do Pintor de tela da Web*.

Relatórios de detalhes e de resumo

O CA SDM tem opções de geração de relatório de detalhes e resumo integradas. Você pode selecionar registros específicos para um relatório usando o recurso de pesquisa das janelas de lista. Por exemplo, na janela Lista de solicitação, você pode digitar critérios de pesquisa para criar uma lista de solicitações que pode ser usada para gerar um relatório.

Para imprimir ou exibir relatórios de resumo ou de detalhes, você deve primeiramente selecionar os registros que deseja incluir no relatório. Você também pode imprimir um relatório de detalhes de uma página para cada registro, selecionando Imprimir formulário no menu Arquivo em qualquer página de detalhes. Para imprimir um relatório para um registro recém-criado, você primeiramente deve salvar o registro.

Observação: para obter mais informações sobre o uso de relatórios, consulte a *Ajuda online*.

Relatórios de análise

A guia Administração do CA SDM também fornece os seguintes relatórios de análise integrados para proporcionar uma visão global e detalhada do processo do service desk:

- Relatórios de Solicitação/Ocorrência
- Relatórios de Área de solicitação/Categoria de ocorrência
- Relatórios de Prioridade de área de solicitação/Prioridade de categoria de ocorrência

Você pode exibir o relatório de análise de hoje, dos últimos trinta dias e de um ano até a data de hoje.

Mais informações:

Gerar relatórios de solicitação ou ocorrência (na página 896)
Gerar relatórios de área de solicitação ou categoria de ocorrência (na página 896)
Gerar relatórios de prioridade de área de solicitação ou de prioridade de categoria de ocorrência (na página 897)

Gerar relatórios de solicitação ou ocorrência

Os relatórios de solicitação ou ocorrência fornecem estatísticas de acordo com um período especificado, como o número de solicitações ou ocorrências abertas, o número de solicitações ou ocorrências fechadas, o tempo médio em que estiveram abertas e o tempo médio até serem fechadas. Esse relatório é classificado por data, do registro mais antigo ao mais novo.

Gerar relatórios de solicitação ou ocorrência na interface da web

1. Selecione a guia Administração.
2. Expanda os nós do Service Desk e Análise.
3. Selecione Solicitação ou Ocorrência.
4. Selecione o relatório apropriado baseado no intervalo de tempo que você quer.

Gerar relatórios de área de solicitação ou categoria de ocorrência

Os relatórios de área de solicitação ou categoria de ocorrência fornecem o número de solicitações ou ocorrências abertas no período especificado para cada área de solicitação ou categoria de ocorrência. Esse relatório é classificado alfabeticamente por área de solicitação ou categoria de ocorrência.

Gerar relatórios de área de solicitação ou categoria de ocorrência na interface da web

1. Selecione a guia Administração.
2. Expanda os nós do Service Desk e Análise.

3. Selecione Solicitação ou Ocorrência.
4. Selecione o relatório apropriado baseado no intervalo de tempo que você quer.

Gerar relatórios de prioridade de área de solicitação ou de prioridade de categoria de ocorrência

Os relatórios de prioridade de área de solicitação ou de prioridade de categoria de ocorrência fornecem o número de solicitações ou ocorrências abertas de acordo com sua prioridade no período especificado para cada área de solicitação ou categoria de ocorrência. Esse relatório é classificado por prioridade (da mais alta a mais baixa) e depois alfabeticamente por área de solicitação ou categoria de ocorrência.

Para gerar relatórios de prioridade de área de solicitação ou prioridade de categoria de ocorrência na interface da Web

1. Selecione a guia Administração.
2. Expanda os nós do Service Desk e Análise.
3. Selecione Solicitação ou Ocorrência.
4. Selecione o relatório apropriado baseado no intervalo de tempo que você quer.

Capítulo 19: Gerenciando conhecimento

Esta seção contém os seguintes tópicos:

Gerenciamento de conhecimento (na página 899)
Localizar procedimentos para gerenciamento de conhecimento (na página 900)
Conhecimento e multilocação (na página 900)
Como configurar uma base de conhecimento (na página 901)
Como usar documentos na base de documentos (na página 904)
Pesquisa de conhecimento (na página 911)
Fóruns (na página 912)
Documentos da árvore de conhecimento (na página 912)
Programação de documentos de conhecimento (na página 913)
Acessar exportação/importação (na página 924)
Web Services (na página 940)

Gerenciamento de conhecimento

O gerenciamento de conhecimento refere-se ao conceito de busca, organizar e publicar o conhecimento. O gerenciamento de conhecimento captura informações rápida e eficientemente e então entrega essas informações para um usuário ou grupo. As informações capturadas e disponibilizadas para recuperação são chamadas de base de conhecimento.

Os usuários podem acessar uma base de conhecimento ao usar o mecanismo de pesquisa. O Gerenciamento de conhecimento permite criar e gerenciar o conteúdo que resida em uma base de conhecimento. Defina a categoria e as permissões do documento para usar grupos ou funções. O Gerenciamento de conhecimento ajuda a oferecer soluções para ocorrências complexas aos clientes. O gerenciamento efetivo de conhecimento rapidamente entrega soluções para os clientes através de um processo amigável e fácil de navegar.

Para gerenciar o conhecimento de maneira efetiva, faça o seguinte:

- Crie uma hierarquia de conteúdo significativa.
- Identifique falhas no conhecimento existente.
- Realize atualizações e a manutenção para ajudar a garantir a relevância do conteúdo.
- Meça o valor do conteúdo disponível.

Mais informações:

Configure as restrições da partição de dados do Gerenciamento de conhecimento para permissões com base em função (na página 209)

Localizar procedimentos para gerenciamento de conhecimento

O CA SDM oferece os procedimentos passo a passo para o gerenciamento de conhecimento nesse guia e na *Ajuda online*.

Para encontrar os procedimentos de passo a passo para o gerenciamento de conhecimento na *Ajuda online*.

1. Efetue logon no CA SDM.

   A página principal do CA SDM aparece.

2. Proceda de uma das seguintes maneiras:

   - Clique em Ajuda, Ajuda do menu principal e navegue da *Ajuda online* para Administração, Gerenciamento de conhecimento.

     Os tópicos de Gerenciamento de conhecimento são exibidos e é possível navegar pela hierarquia para localizar as informações desejadas.

   - Clique em Ajuda, Ajuda nesta janela no menu principal.

     A *Ajuda online* aparece é exibe um tópico de ajuda para a página sobre a qual você deseja informações.

Conhecimento e multilocação

Os documentos de conhecimento e as categorias de conhecimento podem ser específicos para um inquilino, compartilhados entre diversos inquilinos ou compartilhados como público. Ao pesquisar um documento de conhecimento, os resultados são limitados aos documentos que podem ser visualizados pelo inquilino associado ao ticket. Os resultados de pesquisa de FAQ são específicos do inquilino. As classificações para os documentos de inquilino públicos devem ser mantidos separadamente por cada inquilino.

É possível administrar as seguintes configurações no nível do inquilino:

- Conteúdo de ação
- Modelos de documentos
- Processo de aprovação do conhecimento
- Documentos recomendados
- Gerenciamento de conhecimento ROI
- Relatórios

Todas as outras configurações de sistema Gerenciamento de conhecimento são administradas globalmente no nível do fornecedor de serviço.

Observação: a multilocação é configurada no Gerenciador de opções usando a guia Administração.

Como configurar uma base de conhecimento

O gerenciamento de conhecimento efetivo consiste em mais do que o desenvolvimento de uma grande base de conhecimento. O gerenciamento de conhecimento também envolve a implementação de processos e procedimentos para manter o conteúdo preciso e relevante.

Para configurar uma base de conhecimento, realize as seguintes tarefas:

1. Analise como a base de conhecimento será usada e seu escopo.
2. Considere quem são os clientes e de qual informação provavelmente eles irão precisar.
3. Desenvolva um plano estratégico que identifique as potenciais ocorrências que podem resultar na necessidade de atendimento ao cliente. Os problemas identificados podem orientar na determinação de que conteúdo deve residir em sua base de conhecimento.
4. Realize o desenvolvimento de sua base de conhecimento. Crie, organize, realize a manutenção e assegure esses dados. É possível realizar todas essas funções usando o Gerenciamento de conhecimento.

Importar exemplo de dados de conhecimento

Os dados de Conhecimento de exemplo do Knowledge Broker, PCHowTo e Right Answers são fornecidos para seu uso.

Para usar os dados de Conhecimento de exemplo, importe-os para o banco de dados do Gerenciamento de conhecimento.

Observação: para obter mais informações sobre dados de exemplo do KT, consulte o *Guia de Implementação*.

Monitoramento da base de conhecimento

É possível monitorar a eficiência da base de conhecimento usando as seguintes ferramentas de relatório. Estas ferramentas permitem exibir as estatísticas sobre a utilidade de seus documentos e sua efetividade na solução de problemas.

Ficha de relatório de conhecimento

Lista as estatísticas para os documentos criados. Cada usuário tem uma Ficha de relatório de documento de conhecimento individual.

Relatórios com base na web

Exibe métricas que descrevem como o conhecimento está atendendo as necessidades do usuário. Alguns dos recursos usados com mais frequência incluem:

- Listagem dos documentos acessados mais frequentemente.
- Exibição das pesquisas de usuário que não retornaram resultados.

Reindexação da base de conhecimento

As seguintes mudanças realizadas nas configurações de pesquisa requerem a reindexação da base de conhecimento usando o utilitário de Reindexação de conhecimento:

- Após importar o conhecimento
- Após alterar as configurações de análise
- Após exclusões em massa
- Quando ocorre uma falha na pesquisa

A reindexação é necessária, pois os documentos existentes não refletem nenhuma das mudanças feitas aos sinônimos, palavras não pesquisáveis, termos especiais e outros parâmetros de pesquisa até serem reindexadas. Todos os novos sinônimos, palavras não pesquisáveis e termos especiais precisam ser reindexados para ajudar a garantir que as pesquisas com palavra-chave da base de conhecimento estejam atualizadas e precisas.

Execute a reindexação de documentos de conhecimento a partir da linha de comando. O arquivo executável para a reindexação de documentos de conhecimento é pdm_k_reindex.exe.

Observação: a reindexação de documentos na base de conhecimento pode ser uma operação que exige tempo, dependendo do tamanho de seu banco de dados. Recomendamos que você execute o utilitário de reindexação de documentos de conhecimento depois de adicionar todas as mudanças.

Configurações de fila de indexação e desindexação para processamento em lote e instantâneo

Tanto a indexação quanto a desindexação executam um processo de lote para incluir um número predefinido de documentos de uma vez. Esses processos de lote são usados para otimização do desempenho. Caso mais documentos sejam incluídos no lote, o desempenho do sistema aumenta.

O número de documentos que podem ser processados é limitado. O limite depende do tamanho dos documentos e dos anexos vinculados. O tamanho do documento é calculado com base no texto puro e seus anexos. Os elementos de formato e imagem não são calculados.

Observação: é possível limitar o tamanho dos anexos ao navegar na Biblioteca de anexos, Repositórios na guia Administração e editar o repositório para definir o Tamanho limite de arquivo (KB).

O tamanho máximo recomendado para o lote é entre 2 e 12 MB (pelo parâmetro EBR_MAX_INDEX_BATCH_SIZE do arquivo NX.env e o tamanho médio de documento).

- Se o tamanho médio de seu documento (incluindo os anexos) for de aproximadamente 0,1 MB, mantenha a configuração padrão no NX.env:

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=128
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=1
  @NX_EBR_INDEX_QUEUE_ONLINE=Yes
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
  ```

  Essa configuração indica que um lote processa 128 documentos, que as execuções de lote têm intervalos de 10 segundos e que ao reindexar, o intervalo de espera entre dos lotes é de 1 segundo.

- Se o tamanho médio de seu documento (incluindo os anexos) for de aproximadamente 0,5 MB, mantenha a configuração padrão no NX.env

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=25
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=10
  @NX_EBR_INDEX_QUEUE_ONLINE=No
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
  ```

  Essa configuração indica que um lote processa 25 documentos, que as execuções de lote têm intervalos de 10 segundos e que ao reindexar, o intervalo de espera entre dos lotes é de 10 segundos.

Como usar documentos na base de documentos

Os documentos de conhecimento fornecem informações sobre o conhecimento armazenado na base de conhecimento. Criar um conhecimento de qualidade requer a entrada de diversas pessoas. Cada pessoa é responsável por realizar tarefas específicas ao longo dos diversos estágios no ciclo de vida de um documento de conhecimento. Os documentos de conhecimento residem na base de conhecimento e são gerenciados como parte dos seguintes processos em andamento:

1. Identificar o conteúdo para incluir na base de conhecimento.

2. Criar um documento de conhecimento.

   Os documentos de conhecimento são alocados em categorias que algumas organizações atribuem a proprietários.

   Observação: quando um documento é criado ou atualizado, ele é colocado em uma Caixa de entrada de proprietário. Até que os itens sejam publicados, os itens na caixa de entrada não podem aparecer como resoluções e não são adicionados à base de conhecimento.

3. Revise o documento.

   Após um documento chegar à pasta Caixa de entrada no gerenciador de filas, os usuários podem executar as tarefas atribuídas, modificando os documentos de acordo com suas funções atribuídas.

   Todos os usuários com permissão completa (gravação/leitura) para o documento podem modificá-lo. O proprietário atual tem permissões completas para o documento, mas não necessariamente possui permissões explícitas de gravação. Os usuários podem criar versões ou reverter para uma versão anterior quando foi encontrado um problema com o documento.

4. Envie o documento.

   Além do envio a partir da interface de autoatendimento do funcionário ou cliente, o conhecimento também pode ser enviado pelo CA SDM. Essa opção permite ao analista enviar uma nova resolução a partir de um ticket existente. Essa opção também oferece um vínculo entre um problema e sua resolução e pode ajudar aos outros usuários com problemas semelhantes a encontrarem uma solução.

5. Publicar o documento.

   Após um documento ter passado pelo ciclo completo do processo de aprovação, ele pode ser publicado. Um documento que tenha sido publicado torna-se parte da base de conhecimento visível na data de início, que é a data atual por padrão. O documento só é visível por grupos que tenham recebido direitos de acesso para sua leitura. Um usuário com permissões completas pode editar e publicar um documento.

6. Avalie e decida se as seguintes tarefas devem ser realizadas:

   - **Cancelar a publicação do documento—** O proprietário do documento, um gerente de conhecimento ou administrador impede a publicação do documento para fins de edição.

- **Criar uma versão de retrabalho—** Os usuários com permissões de edição completas podem criar uma versão de rascunho de retrabalho de um documento publicado enquanto ele permanece online para exibição e pesquisa. Uma versão de trabalho inicia como uma cópia do documento que é substituído na base de conhecimento depois de ser verificado e republicado.
- **Desativar o documento—** O proprietário do documento, um gerente de conhecimento ou um administrador de sistema pode retirar o documento da base de conhecimento.

As tarefas que são realizadas e quem as realiza pode ser definido para atender a estrutura do processo de aprovação que existe em uma organização.

Observação: é possível acompanhar as atividades de conhecimento a partir da guia Log de evento na página de detalhes do contato. Por exemplo, se um usuário final exibe um documento de conhecimento, o log de evento é atualizado para exibir a ação realizada e um link para o documento. O log de evento também acompanha por quanto tempo o usuário deixou o documento aberto.

Envio de conhecimento a partir do CA SDM

Caso tenha adquirido um conhecimento que acredite que deve ser adicionado à base de conhecimento, é possível enviá-lo para consideração. Além do envio do conhecimento a partir da interface de autoatendimento, o conhecimento também pode ser enviado pelo CA SDM. Um analista pode enviar uma nova resolução a partir de um ticket existente, que oferece um link entre um problema e sua resolução. Além disso, isso pode ajudar aos outros usuários com problemas semelhantes a encontrarem a resolução. Em uma organização que pode ter centenas de tickets abertos simultaneamente, isso pode reduzir um tempo precioso.

Todos os documentos de conhecimento devem ser atribuídos a uma categoria de conhecimento. Se uma Área de incidente/solicitação no CA SDM corresponder às categorias de conhecimento no Gerenciamento de conhecimento, a categoria para o envio de conhecimento é automaticamente selecionada.

Envio de conhecimento a partir do Autoatendimento

Por padrão, qualquer usuário que esteja logado no Gerenciamento de conhecimento pode enviar conhecimento para consideração a partir da página Enviar conhecimento. Essa página permite que o cliente envie conhecimento sem entrar em contato com o representante da central de serviços local. Após enviar o conhecimento, ele passa pelo processo de publicação, em que é revisado e editado antes de ser adicionado à base de conhecimento.

É importante digitar as informações em todos os campos exibidos na página Enviar conhecimento. Tenha bastante atenção ao preencher o campo Resumo. Normalmente, esse campo contém uma breve visão geral do documento que está sendo enviado.

Atributos de documento

Definir os atributos do documento ajuda a gerenciar os documentos em seu pool de conhecimento. Os atributos do documento podem ser atualizados para atribuir um novo especialista no assunto ou proprietário do documento. É possível ainda especificar a data em que o documento é disponibilizado na base de conhecimento e a data em que ele expira. Ao selecionar diferentes modelos de documento, é possível modificar a aparência de cada documento.

Permissões do documento

É possível definir, visualizar e editar as permissões para um documento. Essas permissões podem ser atribuídas a diferentes grupos de pessoas. Ao definir as permissões, é possível decidir por herdar as permissões da categoria principal de um documento ou especificar novas permissões. Por padrão, os documentos herdam as permissões de sua categoria principal. Esse padrão trata das permissões de acesso no nível da categoria ao invés de no nível do documento.

Importante: Ao criar um documento de conhecimento, assegure-se de que as permissões do documento incluam usuários que posteriormente possam ser atribuídos no documento pelo processo de aprovação. Quando um grupo é atribuído a um documento, usuários desse grupo podem não ter a permissão de exibir o documento. Se o documento for atribuído a um usuário específico, restrições de partição de dados padrão permitirão que o usuário exiba o documento.

Edição de resolução

É possível criar documentos de conhecimento com o Gerenciamento de conhecimento usando o Editor de HTML. Esse recurso permite modificar o campo Resolução de um documento de conhecimento no formato WYSIWYG (*What You See Is What You Get - O que você vê é o que você tem*). Usar o Editor de HTML melhora o processo de autoria ao permitir a criação de documentos sem digitar o código HTML, formatar o texto, inserir gráficos e tabelas e criar links para outros documentos. Essas ações aceleram o processo de criação e também oferecem um método fácil para editar um documento para fins organizacionais.

O Editor de HTML permite fazer o seguinte:

- **Exibir o código HTML—** As guias O Modo de design e Modo de origem na barra de ferramentas do Editor de HTML permite alternar entre as diferentes exibições.
- **Formatar o texto—** É possível digitar o Texto do documento diretamente na janela do Editor de HTML. É possível então formatar o texto usando a barra de ferramentas e opções de menu.
- **Inserir gráficos —** é possível inserir um gráfico em seu texto HTML ao selecionar uma imagem na biblioteca de imagens ou ao efetuar o upload de seus próprios gráficos.
- **Inserir tabelas —** em um documento de conhecimento, é possível exibir grandes quantidades de informações de maneira clara para os usuários. É possível usar as tabelas para formatar tais informações em colunas e linhas.
- **Inserir hiperlinks para outros documentos —** é possível inserir hiperlinks para documentos de conhecimento ao criar ou alterar um documento de conhecimento. Dessa forma, um documento de conhecimento pode ser vinculado a outros documentos ou URLs relevantes. Quando o Editor de HTML é usado no Modo de design, os hiperlinks são exibidos como texto azul e sublinhado.
- **Inserir conteúdo de ação —** é possível inserir um Conteúdo de ação (URL ativa) no campo Resolução de um documento de conhecimento que, ao ser clicado pelo usuário, cria um incidente ou executa outra ação.

Preparação de publicação de documento

Após enviar um documento de conhecimento, ele deve ser preparado para publicação ao configurar seus atributos e permissões. Atribuir controles como configurações e categorias é importante para ajudar a organizar os documentos de uma maneira eficiente.

Mais informações:

Como usar documentos na base de documentos (na página 904)
Atributos de documento (na página 907)
Permissões do documento (na página 907)

Publicação de documento

Após um documento ter passado pelo ciclo completo do processo de aprovação, ele pode ser publicado. Um documento que tenha sido publicado torna-se parte da base de conhecimento visível na data de início, que é a data atual por padrão. O documento só é visível por grupos que tenham recebido direitos de acesso para sua leitura.

Quando um documento de conhecimento é publicado, o usuário normalmente não tem permissão para modificar o documento, a menos que a publicação seja cancelada primeiro. Depois disso, é possível fazer modificações. Durante esse período, o documento de conhecimento estará offline e indisponível para os usuários. O proprietário do documento, um gerente de conhecimento ou um administrador de sistema pode cancelar a publicação de um documento ao usar o botão Retrabalho e a caixa de seleção Cancelar publicação. O cancelamento da publicação de um documento faz com que ele volte para o status de rascunho. Um usuário administrativo pode, então, selecionar a próxima etapa no processo de fluxo de trabalho.

Documentos de versão

Usando as capacidades de controle de versão de documentos do Gerenciamento de conhecimento, um analista com privilégios de edição pode criar uma versão de *Retrabalho-rascunho* de um documento. Uma versão de trabalho inicia como uma cópia do documento que é substituído na base de conhecimento depois de ser verificado e republicado. Nesse caso, não há necessidade de cancelar a publicação do documento primeiro.

Usuários com privilégios de edição também podem realizar as tarefas de controle de versão a seguir:

- Salvar uma versão de rascunho de um documento.
- Reverter a uma versão anterior se ocorrer um problema com a versão atual (Rascunho ou Publicado). A guia Versões na página Atualizar documento é o local em que os usuários podem selecionar diferentes versões para reversão para substituir a versão atual.
- Acompanhar o número de versões de documento que são salvas, excluídas e arquivadas na base de conhecimento.

A caixa de entrada de Documentos de conhecimento no Gerenciador de filas do CA SDM é o repositório para documentos com qualquer status, incluindo documentos salvos e atribuídos de retrabalho-rascunho e de rascunho.

Como gerenciar versões de documento

Os administradores podem definir e gerenciar versões de documento realizando as seguintes etapas:

1. Identificar quem pode editar documentos publicados e criar versões para Retrabalho-rascunho. A função em uso para um determinado registro de contato controla os privilégios de edição.
2. Definir um modelo de processo de aprovação que agrupa tarefas ou etapas a serem completadas durante o ciclo de vida de um documento. Por padrão, um modelo de processo de aprovação interno permite que os usuários criem documentos.
3. Determinar se deverá ser usado o processo de aprovação de documento. Os analistas com permissão para ignorar o processo de aprovação podem identificar as tarefas que eles querem iniciar ao criar uma versão para retrabalho-rascunho.
4. Criar regras de arquivamento e eliminação para manutenção de versão de documento.

Expiração de documento

Quando um documento publicado alcança sua data de expiração, o produto geralmente o desativa (isto é, remove o documento da base de conhecimento e do processo de aprovação).

Arquivamento e eliminação de documento

É possível gerenciar o tamanho de seu pool de conhecimento usando o Arquivo morto e Limpar, que remove os documentos antigos e não usados automaticamente. O arquivamento e eliminação melhoram a eficiência de pesquisas de conhecimento ao retornar apenas documentos atuais.

O Arquivamento e eliminação são executados como processos de segundo plano e remove automaticamente registros inativos no banco de dados do CA SDM de acordo com as regras configuradas por você. Essas regras atuam nos objetos do CA SDM em intervalos de tempo específicos.

Pesquisa de conhecimento

O Gerenciamento de conhecimento oferece aos usuários as seguintes opções para recuperar o conhecimento:

Procura de categoria

Encontroa soluções com base nas categorias. Em cada categoria, as subcategorias adicionais podem refinar os resultados de pesquisa para um conjunto de soluções que provavelmente são mais relevantes para uma ocorrência.

Árvore de conhecimento

Faz diversas perguntas para guiar o usuário até as soluções possíveis. As respostas levam as pessoas a uma solução que aparentemente é a mais relevante.

Marcador

Oferece acesso aos documentos visualizados com frequência que estão inclusos em uma lista de marcadores.

Fóruns

Os fóruns permitem que você comunique sobre as ocorrências existentes. O uso de fóruns permite que documentos sejam compartilhados globalmente ou entre grupos predefinidos que trabalham juntos no compartilhamento do documento e nas discussões sobre os desafios existentes.

Os fóruns ampliam o escopo das contribuições de conhecimento, permitindo comunicações sobre dúvidas gerais, dicas de uso e assim por diante. É possível criar um fórum a partir da guia Conhecimento e a partir de um ticket da central de serviços.

Documentos da árvore de conhecimento

O Criador de árvore de conhecimentos é uma ferramenta visual usada para criar árvores de documentos de conhecimento rapidamente e facilmente. Uma árvore de conhecimento é uma representação de conhecimento especializado em uma determinada área. O Criador de árvore de conhecimentos permite aos analistas e engenheiros de conhecimento criar árvores detalhadas que orientam o usuário por uma série de perguntas e respostas possíveis até que eles alcancem uma resolução. Essa ferramenta elimina a necessidade de geração de script especializado ou habilidades de programação e pode envolver apenas um analista trabalhando com um especialista no assunto para criar um design de árvore.

As árvores de documentos de conhecimento podem ter um design complexo. Então, é recomendada a criação de um diagrama para mapear o design antes de criar uma árvore de conhecimento. O diagrama deve conter diversas questões, possíveis respostas e resoluções relacionadas. A hierarquia de perguntas e respostas no diagrama em construção é a base sobre a qual a árvore de documentos de conhecimento será criada.

Após planejar o diagrama de sua árvore de conhecimento, construa a árvore usando o Criador de árvore de conhecimentos.

Programação de documentos de conhecimento

A programação dos documentos de conhecimento oferece aos gerentes de mudanças, gerentes de conhecimento e aos analistas de nível 2 uma exibição de alto nível dos eventos chave no ciclo de vida do gerenciamento de conhecimento. Os seguintes eventos podem ser programados para um documento de conhecimento:

- Envio
- Publicação
- Revisar
- Expiração

A guia de Cronograma de gerenciamento do conhecimento exibe um formato de calendário semelhante ao do Calendário de mudanças, mas em vez de mostrar os horários de início e término, ele exibe apenas datas específicas.

Configurar as exibições de programação (na página 769)envolve a definição de instruções de macro.

O cronograma de documento de conhecimento também pode ser exportado no formato iCalendar.

Observação: ao exportar cronogramas em alguns programas de calendário, selecionar a opção Abrir em vez de Salvar faz com que o arquivo seja importado de maneira incorreta. Para evitar esta ocorrência nos programas de Gerenciamento de conhecimento e Requisição de mudança, selecione a opção Salvar em vez de Abrir. Após salvar o arquivo exportado, importe-o usando a interface do programa de calendário.

Filtro de cronograma de documento de conhecimento

O Filtro de cronograma de documento de conhecimento exibe os seguintes campos:

Inquilino

Filtra a pesquisa por inquilino. Esse campo é exibido para um usuário privilegiado em uma instalação de multilocação.

Tipo de evento

Filtra a pesquisa pelos seguintes tipos de evento:

- Envio
- Revisar
- Publicação
- Desativação

Data de início do cronograma

Especifica a data para o início de um intervalo para filtrar o histórico para exibir apenas as entradas para um intervalo de tempo especificado.

Data final do cronograma

Especifica a data para especificar o término de um intervalo para filtrar o histórico para exibir apenas as entradas para um intervalo de tempo especificado.

Programar fuso horário

Especifica um fuso horário para exibir os resultados da pesquisa.

Observação: se nenhum fuso horário for selecionado, os eventos serão exibidos no seu fuso horário atual.

Proprietário

Define o nome do contato com a atribuição de cuidar da manutenção do documento. Insira o nome do contato no formato "sobrenome, nome" ou abra a caixa de diálogo Pesquisa de contato para localizar e selecionar um contato.

Responsável

Define o nome do contato com responsável por processar o registro. Insira o nome do contato no formato "sobrenome, nome" ou abra a caixa de diálogo Pesquisa de contato para localizar e selecionar um contato.

Especialista

Define o nome do contato com conhecimento no assunto do documento. Insira o nome do contato no formato "sobrenome, nome" para abrir a caixa de diálogo Pesquisa de contato para localizar e selecionar um contato.

Status

Selecione um dos status de documento a seguir para realizar sua pesquisa:

- Rascunho
- Publicado
- Desativado

Categoria

Define a categoria pela qual filtrar documentos recuperados. Insira o nome da categoria na caixa ou abra a janela de Pesquisa de categoria. Quando você clica em Pesquisar, o produto retorna somente documentos associados com a categoria especificada.

Exibição inicial

Selecione a exibição de Knowledge Management Calendar que deseja consultar:

Mês

Exibe um calendário para o mês todo que inclui a data de início de implementação mais antiga especificada no campo Data de início. O calendário mostra informações abreviadas sobre cada mudança dentro da faixa (número de mudança, hora de início e término e primeiro IC afetado).

Semana

Exibe sete dias consecutivos em uma única coluna, iniciando com a data de início de implementação mais antiga especificada no campo Data de início. O calendário inclui informações resumidas sobre cada mudança dentro da faixa especificada (número de mudança, hora de início e término, descrição resumida, responsável, grupo e os primeiros dez ICs afetados).

Dia

Mostra uma exibição semelhante à da semana, exceto por exibir apenas o dia especificado no campo Data de início.

***n* dias**

Mostra uma exibição similar à exibição de semana, exceto pelo fato de continuar para o número de dias especificado.

Lista

Exibe uma página de lista do CA SDM padrão.

Observação: é possível clicar no ícone Mais para exibir o campo Argumentos de pesquisa adicionais. Este campo é destinado apenas a usuários avançados que compreendem SQL e Majic e podem usá-lo para especificar argumentos de pesquisa que não estão disponíveis nos campos de filtro de pesquisa padrão. Você pode digitar uma cláusula SQL WHERE neste campo para especificar um argumento de pesquisa adicional.

Knowledge Schedule Views

A programação dos documentos de conhecimento possui as seguintes exibições:

Mês

Exibe um calendário para o mês todo que inclui a data de início de implementação mais antiga especificada no campo Data de início do cronograma. O calendário mostra informações abreviadas sobre cada mudança dentro da faixa (número de mudança, hora de início e término e primeiro IC afetado).

A programação dos documentos de conhecimento possui uma funcionalidade semelhante à exibição de Change Orders Month com as seguintes exceções:

- Os eventos de conhecimento possuem apenas uma data (não um horário) e um tipo de evento os agrupa, de maneira semelhante às requisições de mudança que são agrupadas por cada período de tempo e tipo de mudança.
- Os tipos de evento possuem as seguintes cores predefinidas padrão, usando as macros schedGroup:
  - Envio - Preto
  - Verificação - Verde
  - Publicação - Azul
  - Desativação - Vermelho

Observação: caso encontre uma data de verificação passada, isso indica que provavelmente ela não foi realizada.

Semana

Exibe sete dias consecutivos em uma única coluna, iniciando com a data de início de implementação mais antiga especificada no campo Data de início do cronograma. O calendário inclui informações resumidas sobre cada mudança dentro da faixa especificada (número de mudança, hora de início e término, descrição resumida, responsável, grupo e os primeiros dez ICs afetados).

Dia

Mostra uma exibição semelhante à da semana, exceto por exibir apenas o dia especificado no campo Data de início do cronograma.

***n* dias**

Mostra uma exibição similar à exibição de semana, exceto pelo fato de continuar para o número de dias especificado.

Lista

Exibe uma página de lista do CA SDM padrão.

Programando configuração de exibição

Você configura as exibições de programação mensal e semanal especificando declarações pdm_macro na seção <head> dos formulários HTMPL que definem a programação. Recomendamos usar a exibição de origem do Pintor de tela da web para editar estes formulários.

Qualquer formulário que exiba uma programação deverá conter o seguinte:

- Uma macro schedConfig
- Pelo menos uma macro schedAttr
- Pelo menos uma macro schedGroup

As macros de configuração estão em um arquivo de origem separado referenciado por uma declaração pdm_include no arquivo de origem principal. Este arquivo permite configurar sua programação sem modificar o arquivo de origem principal.

Por exemplo, as macros de configuração para o formulário Calendário de mudanças, list_chgsched.htmpl, estão em um arquivo chamado list_chgsched_config.htmpl. Para a Programação do ciclo de vida do conhecimento, é possível modificar list_kdsched_config.htmpl usando as mesmas macros.

É possível localizar list_chgsched_config.htmpl e list_kdsched_config.htmpl no seguinte diretório:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

Macro schedConfig — Configurar programação

A macro schedConfig especifica que um formulário contém uma programação e fornece informações básicas de configuração. Os seguintes valores são argumentos válidos da macro:

autosearch=1|0

Especifica se o formulário de programação recarrega dados do servidor quando o usuário selecionar uma exibição fora do intervalo de data selecionado atualmente. Definir o valor para 1 (padrão) faz com que o formulário pesquise automaticamente quando o usuário seleciona uma exibição com um ou mais dias fora do intervalo de seleção de data do filtro de pesquisa. Definir o valor para 0 exige que o usuário pressione o botão Pesquisar para iniciar uma pesquisa.

defaultView=0|1|7|30|99

Especifica a exibição padrão para o filtro de pesquisa como 0 (lista), 1 (dia), 7 (semana), 30 (mês), ou 99 (n-dias).

A especificação para defaultView afeta apenas a exibição inicial do filtro de pesquisa. Após a exibição da programação, o CA SDM mantém automaticamente a seleção de exibição do filtro alinhada com a exibição atual.

Padrão: 30

firstday=0|1|2|3|4|5|6|7

Especifica o primeiro dia da semana na exibição mensal como um número entre 0 (domingo) e seis (sábado).

Padrão: 0

export=xxx|0

Especifica o nome de código do modelo usado para exportação no formato iCalendar. Definir o valor para 0 indica que o recurso e o botão de exportação estão desativados.

Padrão: ChangeSchedule.

legend=1|2|0

Especifica o local da legenda da programação mostrando o nome e a formatação dos grupos na programação. É possível definir o valor para 1 para posicionar a legenda acima da programação, ou 2 para posicioná-la abaixo da programação. Defina o valor para 0 para desativar a legenda.

Padrão: 2

maxGroups=0/*n*

Especifica o número máximo de grupos a serem exibidos em uma única célula da exibição mensal do calendário.

Se houver mais do que maxGroups programados para um único dia, o CA SDM exibe somente os primeiros maxGroups-1, e substitui o último com um hiperlink "..nn more changes" em que o usuário pode passar o mouse por cima ou clicar para ver a lista completa. Defina o valor para 0 para desativar este recurso e permitir um número ilimitado de eventos em uma célula do calendário.

Padrão: 4

nday=(n,n,...)

Especifica seleções para a lista suspensa para a exibição de n-dias.

A especificação é uma lista de contagens de dias que devem ser incluídos na lista suspensa, ou 0 para indicar que a lista suspensa de n-dias é suprimida da programação. O primeiro valor especificado é o padrão para a lista suspensa.

Padrão: (3,7,14,28)

round=(*hr,min*)|0

Especifica se as datas de início e término da programação são arredondadas ao coletar requisições de mudança ou documentos de conhecimento em grupos. Especifique round=0 para desativar o arredondamento.

Por padrão, as datas de início e término da programação agrupam objetos. Todas as datas no CA SDM incluem um horário e, sem arredondamento, objetos programados com uma diferença de até mesmo um minuto ficariam em grupos separados. O arredondamento determina o grupo após ajustar a data inicial para uma hora ou minuto mais cedo e a data de término para uma hora ou minuto mais tarde.

O valor de arredondamento especifica uma hora ou um minuto (mas não ambos). As horas são arredondadas para o múltiplo mais próximo do valor especificado, por exemplo:

round=(0,15) arredonda para o quarto de hora mais próximo

round=(0,30) arredonda para a meia hora mais próxima

round=1 arredonda para a hora mais próxima

round=12 arredonda para a metade do dia mais próxima (12:00 ou 00:00)

round=24 arredonda para o dia mais próximo

Padrão: (0,15)

timefmt=24hr|([am],[pm])

Especifica o formato das horas nas exibições de calendário da programação.

O valor padrão de 24h especifica que as horas são exibidas no formato 24 horas (0:01 - 23:59). O valor alternativo de (am,pm) especifica um sufixo para horários da manhã e tarde, ou ambos.

Observação: todos os argumentos schedConfig são opcionais.

Macro schedAttr — Especificar um atributo armazenado

A macro schedAttr especifica um atributo armazenado para cada item selecionado na lista. Atributos armazenados estão disponíveis ao passar o mouse sobre as informações na exibição mensal; para as informações detalhadas ou resumidas em outras exibições e na função JavaScript setSchedEvents(). Os seguintes valores são argumentos válidos da macro:

attr=xxxx

(Obrigatório) Especifica um atributo do objeto na programação, como uma requisição de mudança ou Documento de conhecimento. Os atributos com pontos são permitidos. O nome de atributo da palavra-chave CI*nn* pode ser usado no Calendário de mudanças para especificar que os primeiros *nn* ICs associados à requisição de mudança estão incluídos nas informações armazenadas.

Observação: este argumento é o único argumento obrigatório para a macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Armazena o atributo da tabela armazenada referenciada para um atributo SREL (ignorado para atributos não SREL). O nome do atributo especificado deve ser precedido por um ponto.

Padrão: .COMMON_NAME

label=

Exibe um rótulo para o atributo na exibição de n-dias.

Padrão: o Majic DISPLAY_NAME do atributo

ident=1|0

Especifica se o atributo é um identificador para o objeto (como um número de referência de uma requisição de mudança). Atributos de identificador são exibidos sem um rótulo à frente do nome do grupo que é exibido ao passar o mouse e na exibição de n-dias.

Padrão: 0

detail=1|0

Especifica se o atributo está incluído nas informações de detalhe mostradas em outras exibições que não mensais. Informações de detalhe são as informações mostradas quando a caixa de seleção Summary Only na exibição não está selecionada..

Padrão: 1

hoverInfo=1|0

Especifica se o atributo é incluído no pop-up de informação suspensa que é mostrado na exibição mensal quando o cursor do mouse é passado sobre um grupo, ou o usuário pressionar Alt+seta direita quando o foco estiver no grupo.

Padrão: 0

summary=1|0

Especifica se o atributo está incluído nas informações de detalhe mostradas em outras exibições que não mensais. Informações de detalhe são as informações mostradas quando a caixa de seleção Summary Only na exibição não está selecionada..

Padrão: 0

Observação: o CA SDM exibe atributos em informações resumidas, detalhadas ou que são exibidas ao passar o mouse na mesma ordem que suas macros schedAttr.

Macro schedGroup—Especificar um grupo de eventos

A macro schedGroup especifica o nome e o código de cores de um grupo de itens. A exibição mensal agrega todos os itens de um grupo em um único evento. Exibições que não a mensal exibem itens individuais no formato para o grupo a que pertencem. Os seguintes valores opcionais são argumentos válidos da macro:

grpname=xxx

(Obrigatório) Especifica o nome do grupo. A macro atribui automaticamente um número ao grupo e atribui o número a uma variável de JavaScript com um nome do formulário schedGroup_xxx, em que xxx é o nome do grupo. Esta variável pode ser usada na função JavaScript setSchedEvents() para criar um evento que pertença ao grupo.

Observação: este argumento é o único argumento obrigatório para a macro schedGroup.

label=xxx

Especifica um rótulo para o grupo. Se especificado, o rótulo é mostrado em todas as exibições.

legend=xxx|0

Exibe uma descrição do grupo para a legenda que é exibida na parte inferior da programação. Os grupos são mostrados na legenda se pelo menos um exemplo do grupo existir na exibição atual. Especificar 0 faz com que o grupo seja sempre excluído da legenda.

Padrão: 0

color=black|*color*

Especifica a cor do texto em itens deste grupo. É possível especificar a cor no formato CSS, seja uma cor web válida ou um valor hexadecimal precedido pelo símbolo #.

Exemplo: insira "#FF0000" ou "red" para vermelho.

Padrão: black

bgcolor=white|*color*

Especifica a cor do plano de fundo para itens deste grupo. É possível especificar bgcolor no formato CSS, seja uma cor web válida ou um valor hexadecimal precedido pelo símbolo #.

Exemplo: insira "#FF000" ou "red" para vermelho.

Padrão: white.

style=normal|bold|italic

Especifica o estilo do texto deste grupo no estilo normal, negrito ou itálico.

Padrão: normal.

A função JavaScript setSchedEvents()

A função JavaScript setSchedEvents() cria eventos na programação. Modifique esta função quando desejar exibir quaisquer objetos novos do grupo. Os objetos predefinidos do grupo são exibidos por padrão.

O CA SDM chama setSchedEvents() uma vez para cada objeto (requisição de mudança ou documento de conhecimento) selecionado pelo filtro de pesquisa da programação. A função cria eventos para o objeto chamando uma segunda função, schedEvent() e passando para a ID do grupo, data de início e data de término do evento.

A função pode criar qualquer número de eventos (incluindo zero) para um objeto. A função padrão setSchedEvents() para o Calendário de mudanças (list_chgsched.htmpl) cria um evento para cada requisição de mudança e agrupa requisições de mudança por tipo de mudança. Esta função é codificada da seguinte forma:

```
1.      function setSchedEvents( chg )
2.      {
3.      var grpnum;
4.      switch( chg["chgtype"] - 0 ) {
5.              case 100: grpnum = schedGroup_std;  break;
6.              case 300: grpnum = schedGroup_emer; break;
7.              default:  grpnum = schedGroup_norm; break;
8.      }
9.      chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.     }
```

O parâmetro case especifica a ID do tipo de mudança. Para listar as IDs de caso, consulte Criar um tipo de mudança.

A função possui um único argumento de um objeto JavaScript contendo os atributos especificados pelas macros schedAttr. O comando switch nas linhas 4-8 examina o atributo chgtype da requisição de mudança e atribui o número de grupo apropriado a partir de uma das variáveis schedGroup_xxxx definidas pelas macros schedGroup anteriores. Na linha 9, ele chama a função schedEvent() para criar um evento na programação, passando o número do grupo anteriormente atribuído e as datas de início e término da programação. As datas estão disponíveis no objeto do argumento porque foram especificadas nas macros schedAttr anteriores.

Acessar exportação/importação

A ferramenta de importação/exportação de conhecimento migra e sincroniza os dados entre diferentes sistemas Gerenciamento de conhecimento e permite exportar/importar Documentos de conhecimento. Use esta ferramenta para definir transações de exportação/importação.

Observação: caso a multilocação esteja instalada, todas as categorias públicas e de inquilino que foram importadas de um sistema anterior são exibidas como públicas no novo sistema de multilocação, mas os documentos importados podem ser específicos de inquilinos.

Para acessar a página do KEIT, navegue em Conhecimento, Documentos, Exportar/importar na guia Administração.

A opção Exportar/importar é exibida e contém os seguintes elementos:

Exportar transações

Mostra uma lista de exportações.

Modelos de exportação/importação

Exibe uma lista de modelos que podem ser editados.

Importar

Mostra uma lista de pacotes disponíveis para importação.

Importar transações

Mostra uma lista de importações.

Observação: Ao importar ou exportar conhecimento da interface da web, o Gerenciamento de conhecimento usa a Função do utilitário da linha de comando padrão, e não a função atual na qual o usuário está conectado ao CA SDM. O padrão da Função do utilitário da linha de comando é definido no tipo de acesso para o usuário.

Como importar/exportar conhecimento

Exporta/Importar modelos permite definir uma transação de importação/exportação.

Para exportar ou importar o conhecimento, faça o seguinte:

1. Proceda de uma das seguintes maneiras:
   - Crie um modelo de Exportação/importação para criar um pacote de Exportação.
   - Use um modelo de Exportação/importação existente para criar um pacote de Exportação.
2. Exporte os dados para outro sistema ao realizar uma das seguintes ações:
   - Clique Exportar na página Detalhes do modelo.
   - Na página Transação de exportação, clique com o botão direito do mouse em uma transação e clique em Repetir no menu de atalho.
   - Usar o utilitário pdm_ket (na página 937)
3. Importe os dados de conhecimento do pacote ao realizar uma das seguintes ações:
   - Copie o pacote de conhecimento para uma instalação CA SDM direcionada e coloque-a no diretório $NX_ROOT/site/keit/import.
   - Na página Lista de pacotes de importação de conhecimentos, clique com o botão direito do mouse no Pacote de conhecimento e clique em Importar no menu de atalho.
   - Na página Transação de importação, clique com o botão direito do mouse em uma transação e clique em Repetir no menu de atalho.
   - Usar o utilitário pdm_kit_txt (na página 938)

Observação: O nome do pacote de conhecimento deve iniciar com o prefixo "package_" para que seja listado na página Importar conhecimento.

Importante: O utilitário de importação r11.0 foi renomeado para pdm_kit_txt.exe para permitir a importação de arquivos de texto do r11.0. Esse utilitário não oferece suporte a nenhum dos aprimoramentos de importação da r12.0.

Mais informações:

Exportar/importar pacotes (na página 928)

Exportar transações

É possível classificar as transações por pacote, modelo e status. Todas as transações KEIT são registradas nos seguintes arquivos de log:

stdlog

Registra informações do CA SDM.

keitstat.log

Oferece informações estatísticas sobre a operação do KEIT.

keitinfo.log

Oferece informações detalhadas sobre a operação do KEIT.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

A página Exportar transações contém os seguintes campos:

Pacote

Exibe o nome do pacote de exportação.

Executado por

Exibe o usuário que realizou a exportação.

hora de início

Mostra o horário de início da transação.

Hora de término

Mostra o horário de término da transação.

Contagem de documentos

Exibe o número de documentos exportados.

Contagem de falhas

Exibe o número de exportações com falha.

Andamento (%)

Mostra o andamento da transação.

Status

Mostra o status da transação.

Importar transações

A página Importar transações permite que as transações sejam classificadas por pacote, modelo e status ao clicar em qualquer uma das colunas.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

A página contém os seguintes campos:

Pacote

Exibe o nome do pacote de importação.

Executado por

Exibe o usuário que realizou a importação.

hora de início

Mostra o horário de início da transação.

Hora de término

Mostra o horário de término da transação.

Contagem de documentos

Exibe o número de documentos importados.

Contagem de falhas

Exibe o número de importações com falha.

Andamento (%)

Mostra o andamento da transação.

Status

Mostra o status da transação.

Mais informações:

Mostrar configurações de importação (na página 933)

Exportar/Importar documentos

Para migrar e sincronizar os dados entre diferentes sistemas Gerenciamento de conhecimento, use o KEIT na Administração do conhecimento, que permite importar e exportar documentos de conhecimento.

É possível criar modelos do KEIT para definir uma transação de importação/exportação.

Observação: para importar dados de conhecimento do r11.0, use o utilitário pdm_kit-txt.

Exportar/importar pacotes

A sintaxe a seguir nomeia os pacotes de exportação:

- Nome do servidor
- Data
- Horário de início

É possível definir os diretórios de pacote ao editar a opção *keit_path* em Gerenciador de opções, Conhecimento. Os pacotes são armazenados nos seguintes diretórios padrão:

- Exportar pacotes

  KEIT_PATH\export

- Importar pacotes

  KEIT_PATH\import

Para adicionar atributos para a disponibilidade de exportação/importação, adicione os seguintes nomes de atributo para o arquivo NX.env:

@NX_KEIT_AVAILABLE_FIELDS

Adiciona o nome do atributo.

@NX_KET_ADDL_FIELDS

Adiciona o nome do atributo e, se o novo atributo for um SREL para outro objeto, adiciona o nome do atributo usado para sincronizar os sistemas de origem e de destino.

Exemplo: adicionar atributos

@NX_KEIT_ADDL_FIELDS =
STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME

Os diretórios de importação e exportação contêm os seguintes arquivos:

keit_config.xml

Contém o arquivo de configuração para um pacote de importação ou exportação.

data.xml

Contém os arquivos de dados contendo os valores dos documentos de conhecimento.

rep.xml

Contém os repositórios que são referenciados no arquivo data.xml.

imagens

Especifica os arquivos de imagem nos documentos de conhecimento.

Exibir modelos de exportação/importação

Os modelos do KEIT são usados para definir as transações de importação/exportação.

Observação: o modelo de importação/exportação padrão é chamado All-Docs e não contém o campo STATUS_ID. Esse modelo cria o arquivo data.xml e importa os documentos com um status de rascunho. Caso adicione manualmente o campo STATUS_ID ao modelo All-Docs antes de exportar a operação, o status do documento original é preservado na importação.

Para exibir Modelos de exportação/importação de conhecimento

1. Clique na guia Administração.

   O Console de administração aparece.

2. Clique em Conhecimento. Documentos.

   Clique em Exportar/Importar, Modelos de exportação/importação.

A Lista de modelos de exportação/importação de conhecimentos é exibida.

3. Clique em um modelo na coluna Nome.

   O modelo KEIT é aberto.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Pesquisar modelos de exportação e importação

É possível pesquisar por um modelo usando a página Knowledge Export/Import Template Settings.

Observação: se multilocação estiver instalada, selecione o inquilino apropriado na lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos. Uma lista suspensa de inquilinos aparece no filtro de pesquisa. Se você selecionar <vazio> nessa lista suspensa, a pesquisa será pública. Uma coluna de inquilinos também aparecerá na página da lista.

Para pesquisar os Modelos de exportação/importação de conhecimento

1. Na guia Administração, navegue até Conhecimento, Documentos, Exportação/importação, Modelos de exportação/importação.

   A Lista de modelos de exportação/importação de conhecimentos é exibida.

2. Clique em Pesquisar e insira seus parâmetros de pesquisa.

   Os resultados da pesquisa são exibidos.

3. Clique em Mostrar filtro.

   O filtro é exibido.

4. Modifique a pesquisa usando as seguintes opções:

   Pacote

   Pesquisar por nome do pacote.

   Data da modificação mais antiga

   Pesquisar por data de modificação mais antiga.

   Data da modificação mais recente

   Pesquisar por data de modificação mais recente.

Argumentos de pesquisa adicionais

Oferece argumentos de pesquisa adicionais.

Os resultados da pesquisa são exibidos.

5. Clique em um modelo nos resultados da pesquisa.

   O Modelo é aberto.

Criar um modelo de exportação/importação

É possível criar e modificar um modelo usando a página Knowledge Export/Import Template Settings na guia Administração.

Para criar um modelo de exportação/importação de conhecimento

1. Na guia Administração, navegue até Conhecimento, Documentos, Exportação/importação, Modelos de exportação/importação.

   A Lista de modelos de exportação/importação de conhecimentos é exibida.

2. Clique em Criar novo.

   A página Criar exportar/importar modelo é exibida.

3. Preencha os seguintes campos:

   Nome do modelo

   Identifica o nome do modelo.

   Descrição

   Fornece uma descrição breve do modelo.

4. Preencha os campos adequados nas seguintes guias:

   - Exportar campos (na página 932)
   - Exportar filtro (na página 933)
   - Importar configurações (na página 933)

   Clique em Salvar.

   O modelo é criado.

Consulte também

Exportar transações (na página 926)
Importar transações (na página 927)

Exibir campos de exportação

Para exibir os campos de exportação, crie um KEIT.

A guia Exportar campos é exibida e contém os seguintes campos:

Disponível

Exibe os campos Documentos de conhecimento que estão disponíveis para exportação.

Observação: se deseja preservar o status dos documentos, como Rascunho, para o processo de exportação e importação, adicione STATUS_ID à coluna Exportado.

Exportado

Especifica os campos do documento a serem exportados.

Exportar anexos

Exporta anexos do arquivo Documento de conhecimento.

É possível usar as setas na seção Selecionar atributos de documento para adicionar exportação de atributos de documento.

Observação: se você editar o modelo de exportação/importação usando o Firefox, o tamanho da lista não é alterado depois de usar as setas na primeira edição. Fechar e abrir novamente o modelo no modo de edição e usar as setas novamente fará com que o tamanho da lista mude. Esse comportamento não ocorre ao usar o Internet Explorer.

Importante: Campos exportados no KEIT têm uma prioridade mais alta do que quando os campos são selecionados como padrão na guia Importar configurações. Se você selecionou um campo de exportação padrão na guia Importar configurações, ele não é processado como o campo padrão.

Exibir o filtro de exportação

Para exibir o filtro de exportação, crie um KEIT (Knowledge Export/Import Template - Modelo de exportação/importação de documento de conhecimento).

A guia Exportar filtro é exibida e contém os seguintes campos:

Categoria

Abre a página Categoria do documento de conhecimento. Use esta opção para adicionar categorias à lista na guia Exportar filtro.

Remover categoria

Remove categorias da lista da guia Exportar filtro.

Clear Category

Limpa a lista de categorias na guia Exportar filtro.

Incluir categorias filho

Exporta documentos de categorias filho de categorias exportadas.

Incluir categorias secundárias

Exporta categorias secundárias de documentos exportados.

Incluir todos os documentos vinculados às categorias selecionadas

Exporta todos os documentos vinculados às categorias selecionadas.

Observação: é ativado apenas se Incluir categorias secundárias for selecionado.

Filtro adicional

Fornece uma cláusula WHERE adicional.

Mostrar configurações de importação

Para mostrar as configurações de importação, crie um KEIT.

A guia Configurar importações contém os seguintes campos:

Limite de erros (%)

Interrompe o processo de importação (define o status como Com falha) caso a porcentagem de erros exceda o número especificado.

Substituir documentos publicados

Permite que os documentos importados substituam os documentos publicados do servidor de destino.

Substituir documentos em todos os status Não publicado

Permite que os documentos importados substituam os documentos não publicados do servidor de destino.

Usar valores padrão ao substituir documentos

Usa os valores padrão em documentos substituídos para os campos definidos.

Indexar documentos imediatamente

Indexa o documento após o processo de importação.

Status

Selecione Rascunho, Publicado ou Desativado.

Prioridade

Define o nível de prioridade das configurações de importação.

Modelo

Seleciona um dos seguintes modelos padrão:

- Interno - Documento de conhecimento
- Interno - Documento da árvore de conhecimento
- Incorporado - Edição rápida

Proprietário

Permite definir o proprietário ao abrir a página de Pesquisa de contato.

Autor

Permite definir o autor ao abrir a página de Pesquisa de contato.

Especialista

Permite definir o especialista ao abrir a página de Pesquisa de contato.

Responsável

Permite definir o responsável ao abrir a página de Pesquisa de contato.

Data de expiração

Abre o auxiliar de data.

Data de revisão

Abre o auxiliar de data.

ID do produto

Permite definir a ID do produto abrindo a página Pesquisa de produto.

Ativo

Abre a página Pesquisa de item de configuração.

Motivo raiz

Abre a página Pesquisa de causa raiz.

Prioridade do Service Desk

Define a prioridade do Service Desk das configurações de importação.

Gravidade

Define o nível de severidade das configurações de importação.

Impacto

Define o nível de impacto das configurações de importação.

Urgência

Define o nível de urgência das configurações de importação.

Editar um modelo de exportação/importação

É possível editar modelos de importação e exportação a partir da página Lista de modelos de exportação/importação de conhecimentos.

Para editar um modelo de exportação ou importação

1. Navegue para Conhecimento, Documentos, Exportar/importar, Modelos de exportação/importação.

   A Lista de modelos de exportação/importação de conhecimentos é exibida.

2. Selecione um modelo

   A página Template Detail é exibida.

3. Clique em Editar.

   Modifique os campos apropriados:

   Nome do modelo

   Identifica o nome do modelo.

   Descrição

   Fornece uma descrição breve do modelo.

4. Modifique os campos apropriados nas seguintes guias:
   - Exportar campos (na página 932)
   - Exportar filtro (na página 933)
   - Importar configurações (na página 933)

5. Clique em Salvar.

   Suas edições são salvas.

Mais informações:

Importar transações (na página 927)

Utilitário pdm_ket—Ferramenta de exportação de conhecimento

O utilitário pdm_ket exporta conhecimento com base em um modelo criado da interface da web a partir de um computador de origem para um pacote de conhecimento.

Os anexos e seus links são exportados para data.xml durante a exportação. Antes de importar os anexos, mova-os manualmente para o seguinte diretório no servidor de destino:

$NX_ROOT/site/attachments/default

Use este utilitário para:

- Criar um arquivo de configuração com base no modelo de exportação de conhecimento relacionado.
- Exportar dados com a UUID do documento, e conteúdo como título, resumo, problema, resolução e outros atributos do documento, como proprietário, status e assim por diante.
- Exportar todas as imagens exclusivas usadas pelos documentos exportados (sempre exportado).
- Exportar todos os anexos exclusivos usados pelos documentos exportados (campo EXP_ATTMNT).

  Os arquivos são copiados do repositório remoto para a pasta do pacote local.

O utilitário é chamado da seguinte forma:

```
pdm_ket -n <template name> [-h] ]-v]
```

-n <template name>

Define o nome do modelo usado para exportar (diferencia maiúsculas de minúsculas).

-h

(Opcional) Exibe a ajuda no utilitário.

-v

(Opcional) Permite ampla geração de logs (bop_logging) de eventos de programa. Esta opção é geralmente usada para resolução de problemas internos.

Exemplo: usando pdm_ket para exportar conhecimento usando o modelo my_template.

```
pdm_ket -n my_template
```

O utilitário pdm_ket pode ser programado usando um agendador de terceiros para exportar Documentos de conhecimento.

Utilitário pdm_kit—Ferramenta de importação de conhecimento

O utilitário pdm_kit importa dados para o servidor de destino de acordo com as definições no arquivo de configuração de um pacote.

Importante: O utilitário de importação da r11.0 foi renomeado para pdm_kit_txt.exe para permitir a importação de arquivos de texto da r11.0. Esse utilitário não suporta nenhum dos aprimoramentos de importação do Release 12.7.

Os dados mencionados anteriormente pelo utilitário pdm_ket obtém o valor verdadeiro da ID ou UUID do servidor de destino. Ao executar o utilitário pdm_kit, um novo parâmetro da id de usuário é aplicado. O utilitário pdm_kit funciona da seguinte forma:

1. Importa documentos substituindo o valor da id de usuário (para contatos) ou nome mencionado (para campos como ativo) com a UUID apropriada do servidor de destino.
2. Importa imagens.
3. Importa anexos.
4. Faz o upload de arquivos da pasta do pacote local para repositórios remotos.

Observação: se a edição de documentos publicados estiver desativada o documento importado é criado como uma versão de retrabalho.

O utilitário é chamado da seguinte forma:

```
pdm_kit [-h] -f -u [-v]
```

-h

(Opcional) Exibe ajuda para o utilitário na interface.

-f

Especifica o caminho para o pacote

-u

Especifica o usuário padrão.

-v

(Opcional) Permite ampla geração de logs (bop_logging) de eventos de programa. Esta opção é geralmente usada para resolução de problemas internos.

Exemplo: usando o pdm_kit para importar um pacote

```
pdm_kit -f c:\package_path -u ServiceDesk
```

Permitir que usuários exportem e importem conhecimento

É possível permitir que os analistas concedam permissões de exportação e importação ao gerenciar sua lista de funções na guia Administração.

Para conceder permissões de exportação/importação

1. Navegue até Gerenciamento de segurança e das funções, Gerenciamento das funções, Lista de funções.

   A Lista de funções aparece.

2. Selecione uma função com o Tipo de interface do analista.

   A página Detalhes da função aparece.

3. Clique em Editar.

   A página Atualizar função aparece.

4. Clique na guia Conhecimento.

   Proceda de uma das seguintes maneiras:

   - Selecione a caixa de seleção Permitir exportação.
   - Selecione a caixa de seleção Permitir importação.
   - Selecione ambas as caixas de seleção.

5. Clique em Salvar.

   A página Detalhes da função é exibida novamente.

6. Revise as mudanças na guia Conhecimento.

   Feche a página Detalhes da função.

É possível também impedir que os usuários exportem/importem ao desmarcar as caixas de seleção na guia Conhecimento da página Detalhes da função.

Web Services

O conhecimento pode ser acessado pelos serviços web SOAP. Há diversos métodos disponíveis, permitindo a pesquisa, recuperação, criação e atualização de documentos e uma série de outras operações.

Observação: para obter mais informações sobre serviços web SOAP, consulte o *Guia de Implementação*.

Capítulo 20: Administrando o Gerenciamento de conhecimento

Esta seção contém os seguintes tópicos:

Administração de conhecimento (na página 941)
Localizar procedimentos para administração de conhecimento (na página 942)
Funções e papéis do Gerenciamento de conhecimento (na página 942)
Como gerenciar os privilégios da função e documentar a visibilidade (na página 956)
Action Content (na página 956)
Processo de aprovação de documentos (na página 962)
Políticas automatizadas (na página 970)
Controle de documento de conhecimento (na página 975)
Categorias de conhecimento (na página 993)
Relatórios e métricas (na página 1004)
Pesquisar (na página 1006)
Opções de integração do CA SDM (na página 1026)
Pesquisa de soluções (na página 1036)
Configurações do sistema Gerenciamento de conhecimento (na página 1039)

Administração de conhecimento

É possível definir as configurações administrativas para o Gerenciamento de conhecimento. É possível definir opções de Conhecimento de autoatendimento (na página 945) para atender as necessidades dos usuários e criar um ambiente efetivo e eficiente para o gerenciamento e entrega de conhecimento. Use a guia Administração para definir as opções de sistema. É possível definir as permissões de conhecimento com base no grupo ou função de um contato. Aplique configurações que podem ajudar a conformidade com a funcionalidade e o uso do Gerenciamento de conhecimento.

Importante: A reindexação de documentos na base de conhecimento e a execução de cálculo para Políticas automatizadas e Ficha de relatório de conhecimento podem ser demoradas. Recomendamos a realização dessas operações fora do horário comercial ou quando seu sistema estiver menos ocupado.

Localizar procedimentos para administração de conhecimento

O CA SDM oferece os procedimentos passo a passo para a administração de conhecimento nesse guia e na *Ajuda online*.

Para encontrar os procedimentos de passo a passo para a administração de conhecimento na *Ajuda online*.

1. Efetue logon no CA SDM.

   A página principal do CA SDM aparece.

2. Proceda de uma das seguintes maneiras:

   - Clique em Ajuda, Ajuda do menu principal e navegue da *Ajuda online* para Administração, Administração de conhecimento.

     Os tópicos de Administração de conhecimento são exibidos e é possível navegar pela hierarquia para localizar as informações desejadas.

   - Clique em Ajuda, Ajuda nesta janela no menu principal.

     A *Ajuda online* aparece é exibe um tópico de ajuda para a página sobre a qual você deseja informações.

Funções e papéis do Gerenciamento de conhecimento

O Gerenciamento de conhecimento foi projetado para uma ampla variedade de usuários, dos administradores e gerentes de conhecimento, que mantêm o produto, aos clientes e funcionários, que usam o sistema para encontrar soluções para seus problemas. Embora uma pessoa possa ter diversas funções, as funções a seguir são as funções de usuário básicas encontradas no Gerenciamento de conhecimento:

- **Cliente—** Um usuário final externo que realiza as tarefas de autoatendimento básicas.
- **Funcionário—** Um usuário final interno que realiza as tarefas de autoatendimento básicas.
- **Analista de conhecimento—** Um usuário que é responsável por uma ou mais etapas no processo de gerenciamento de conhecimento. Esse usuário interage com analistas do service desk para criar e manter uma base de soluções de qualidade.

- **Gerente de conhecimento—** Um supervisor para o Analista de conhecimento. Esta função processa as reatribuições e escalonamentos de documentos de conhecimento e gerencia os aspectos administrativos do dia-a-dia da solução, incluindo criação de estrutura de categorias, gerenciamento de palavras não pesquisáveis, termos especiais, sinônimos e outras definições e opções que são mais dinâmicas do que um administrador de gerenciamento de conhecimento pode controlar.
- **Administrador—** O administrador que possui acesso a todas as funcionalidades nos produtos CA SDM e Gerenciamento de conhecimento em uma única função. Normalmente, essa função é usada ao implementar o CA SDM para ajudar a garantir que todos os usuários e funções sejam definidos de maneira adequada e para um ambiente CA SDM que possui uma única pessoa realizando todas as tarefas de administração.
- **Administrador do gerenciamento de conhecimento—** Um administrador que é responsável por configurar e monitorar o processo de gerenciamento de conhecimento. Essa função inclui a criação da estrutura da categoria, a definição do processo de aprovação e as configurações padrão de pesquisa e segurança.

Os diferentes níveis de acesso estão associados a cada função no ambiente CA SDM. Esse nível ajuda a definir as tarefas que cada função realiza.

Consulte também

Interfaces com o usuário do Gerenciamento de conhecimento (na página 944)
Funções de configuração e gerenciamento do Gerenciamento de conhecimento (na página 944)
Opções de conhecimento de Autoatendimento (na página 945)
Documentos e usuários (na página 952)
Como gerenciar os privilégios da função e documentar a visibilidade (na página 956)

Interfaces com o usuário do Gerenciamento de conhecimento

As interfaces com o usuário a seguir ajudam a gerenciar o conhecimento:

- **Autoatendimento—** Na interface de autoatendimento, os clientes e funcionários usando o CA SDM podem acessar documentos de conhecimento e enviar conhecimento para considerações futuras. Os clientes podem pesquisar, navegar ou usar marcadores para localizar e exibir documentos de conhecimento.
- **Documentos de conhecimento—** Na interface de documentos de interface, acessada a partir do nó de Documentos de conhecimento do Gerenciador de filas do CA SDM, todos os usuários do sistema podem exibir sua Caixa de entrada e comentários de acompanhamento. O *administrador* gerencia seus documentos não atribuídos/não indexados, políticas automatizadas de ciclo de vida de documentos e fóruns de usuários.
- **Gerenciamento de conhecimento—** Na interface de gerenciamento de conhecimento, acessada a partir da guia Conhecimento no CA SDM, o *analista de conhecimento* ou o *gerente de conhecimento* pode encontrar, organizar e publicar o conhecimento. Os analistas também podem filtrar os documentos exibidos usando opções avançadas e classificar os resultados por relevância, data de modificação e muito mais.
- **Administração de conhecimento—** Na interface de administração de conhecimento, acessada a partir do nó de Conhecimento na guia Administração do CA SDM, o *administrador, gerente de conhecimento ou o administrador de gerenciamento de conhecimento* pode definir as opções do sistema. As configurações podem ajudar a estar de acordo com a funcionalidade e o uso do Gerenciamento de conhecimento.

Funções de configuração e gerenciamento do Gerenciamento de conhecimento

É possível realizar as seguintes funções de gerenciamento e configuração no Gerenciamento de conhecimento:

- Criar um "conteúdo de ação" (um URL de ação ao vivo) que pode ser inserido no campo Resolução de um documento.
- Configurar o processo de aprovação e defina o processo do ciclo de vida do documento de conhecimento.

- Configurar as políticas automatizadas que automatizam determinadas tarefas no processo de aprovação do documento de conhecimento.
- Configurar opções de documento relacionadas a comentários, envio de conhecimento, modelos e configurações de documento.
- Criar modelos que controlam a forma como um documento exibe informações.
- Gerenciar o mecanismo de pesquisa Gerenciamento de conhecimento padrão e configurar palavras não pesquisáveis, termos especiais e sinônimos usados para executar pesquisas por palavras-chave e linguagem natural.
- Criar "documentos recomendados" que são exibidos na interface de autoatendimento quando os usuários pesquisam soluções de conhecimento.
- Administrar a estrutura de categoria de conhecimento e acessar documentos mais facilmente.
- Configure a Ficha de relatório de documento de conhecimento e as configurações gerais de sistema.
- Definir pesquisas que coletem e analisem o feedback do cliente sobre o desempenho do documento de conhecimento.
- Gerenciar a integração do Gerenciamento de conhecimento no CA SDM, incluindo o mapeamento de campos e a configuração de pesquisa de solicitações e ocorrências.

Opções de conhecimento de Autoatendimento

Os clientes e funcionários usando o CA SDM possuem acesso aos documentos de conhecimento através da interface de autoatendimento. Os clientes podem pesquisar, navegar ou usar marcadores para localizar e exibir documentos de conhecimento. Fornecer aos clientes o acesso aos documentos de conhecimento e aos serviços permite que os clientes encontrem respostas sozinhos e reduz pressão sobre os recursos.

Na interface com o usuário de autoatendimento, os funcionários e clientes podem exibir as seguintes opções de solução de conhecimento:

- **Procurar por soluções de conhecimento—** Os funcionários e clientes podem inserir palavras-chave e frases em um campo de pesquisa que recupera uma lista de soluções de conhecimento. É possível configurar essa opção no seguinte local: Administração, Conhecimento, Pesquisa, Configurações de pesquisa.

- **Exibir as soluções principais—** Os funcionários e clientes podem exibir uma lista das principais soluções na interface de autoatendimento. A configuração de Administrador: Administração, Conhecimento, Sistema, Configurações gerais, Soluções principais—Número de documentos a serem exibidos, determina o número dos documentos a serem exibidos.
- **Prompt para pesquisa de conhecimento—**Após a abertura de um documento de conhecimento, o usuário pode ler o documento e acessar diversas questões de pesquisa. Uma dessas questões permite que o usuário indique através de um prompt se eles acreditam que seus problemas estão sendo resolvidos. É possível configurar essa opção no seguinte local: Administração, Conhecimento, Pesquisa de soluções, Configurações da pesquisa.
- **Sugerir conhecimento—** Os usuários e clientes podem, onde permitido, exibir uma lista das sugestões de conhecimento ao criarem um ticket na interface de autoatendimento. É possível configurar essa opção no seguinte local: Administração, Conhecimento, Integração com o Service Desk, Sugerir conhecimento.

Pesquisa avançada

Nas Configurações de pesquisa avançadas, os clientes e funcionários podem usar as seguintes opções para refinar uma pesquisa para a solução de um problema:

Pesquisa Gerenciamento de conhecimento

Pesquisa por determinadas palavras-chave, que atuam como correspondências preliminares.

Pesquisa de linguagem natural

Pesquisa por palavras e contas por proximidade de palavra, ordem de palavra e relevância.

Os resultados da pesquisa são listados por relevância. A Relevância é determinada de acordo com os critérios de pesquisa especificados (expressados como EXCELENTE, BOM e assim por diante). Os documentos com a relevância mais alta (EXCELENTE) são relacionados em primeiro lugar.

Cada resultado pode incluir um título que é exibido com um link, um resumo do documento e uma estatística adicional relevante para o documento, como a Classificação de relevância, a ID do documento, Data de modificação, Classificação do FAQ e Ocorrências recebidas.

Dependendo de como o administrador configura o Gerenciamento de conhecimento, os usuários podem abrir um incidente, classificar um documento e fornecer comentários quando um documento de conhecimento estiver aberto.

Informações de documento de conhecimento

Cada documento de conhecimento contém campos de documento chave que fornecem as informações. Dependendo do modelo de documento usado, são exibidos diferentes campos ou eles aparecem diferentes no documento.

Um título identifica o documento. O documento também contém as seguintes informações:

Resumo

Resume o documento, descreve brevemente o problema.

Problema

Descreve o problema.

Resolução

Descreve como resolver o problema no formato HTML ou texto sem formatação.

Consulte também

Lista os documentos que estão relacionados ao documento atual. Caso clique no hiperlink de um documento, uma página à parte contendo o documento relacionado é aberta.

Anexos

Lista os arquivos que estão anexados ao documento e podem ser transferidos por download. Os anexos oferecem informações adicionais sobre o documento.

Categorias relacionadas

Lista as categorias que estão relacionadas ao documento. Caso você clique em um hiperlink de categoria, a página Ferramentas de pesquisa é atualizada para exibir tal categoria.

Tickets relacionados

Links para solicitações, incidentes, problemas, ocorrências e documentos que foram abertos como resultado de um documento ou que foram resolvidos usando um documento.

Propriedades

Indica as propriedades de documento adicionais selecionadas no modelo do documento. Por padrão, a data de modificação e a ID do documento são exibidas.

Comentários

Lista os comentários dos usuários para o documento. Juntamente com os comentários, estão o nome, endereço de email do contato e a data.

Classificar e comentar

Oferece comentários e feedback de acompanhamento sobre se o documento foi útil para responder a dúvida. É possível classificar a utilidade do documento, com base nas seguintes perguntas:

- Este documento resolveu o seu problema?
- Indique o quanto este fórum foi útil.

É possível ainda adicionar um comentário e atribuí-lo a outro analista para acompanhamento usando os seguintes tipos de comentário.

- Link com problemas
- Candidato para publicação
- Candidato para desativação
- Informações incorretas
- Informações ausentes
- Recomendar novo conteúdo
- Revisar
- A solução não funciona

A seção Opções da página permite que você realize os seguintes cursos de ação:

- Editar
- Adicionar/remover indicador
- Assinar
- Classificar e comentar
- Email
- Novo fórum
- Novo incidente
- Novo incidente baseado neste documento
- Versão para impressão

Mais informações:

Criar um tipo de comentário (na página 978)
Configurar políticas de Autoatendimento (na página 1035)

Anúncios

Os anúncios são uma maneira rápida de fornecer soluções para um problema. Os anúncios fornecem uma solução para um problema frequente e para atender às chamadas para a central de serviços.

Os anúncios atuais são exibidos na seção direita da janela principal do CA SDM ao efetuar o primeiro logon no sistema.

Classificar documentos

É possível classificar os documentos em diversas ordens.

Para classificar documentos

1. Na guia Conhecimento, selecione o nó da árvore a partir da lista de categoria na seção esquerda.
2. Expanda o nó e clique em uma categoria.

   A página Lista de documentos aparece.
3. Classifique os documentos usando a lista Ordenar por nas seguintes ordens:
   - Classificação da pergunta freqüente
   - Número de localizações:
   - Documentos modificados recentemente
   - Contagem de soluções

   Os documentos são listados na ordem selecionada.

Navegação em documentos

É possível categorizar os documentos de conhecimento para permitir que os clientes procurem por informações com base nos FAQs. Ao selecionar uma categoria de conhecimento, as subcategorias e os documentos de conhecimento são exibidos. É possível selecionar o documento que gostaria de visualizar ou selecionar uma subcategoria para restringir mais sua pesquisa.

Para melhorar os recursos de autoatendimento, uma lista dinâmica dos documentos usados com mais frequência é exibida.

Observação: os usuários podem especificar um critério sobre um item de interesse e o mecanismo de pesquisa encontra documentos de conhecimento correspondentes e os exibe na página de resultado de pesquisa como um conjunto de links de "documentos recomendados". A consulta da pesquisa pode ser expressa como uma palavra-chave ou um conjunto de palavras (frase) que identifica o conceito desejado que um ou mais documentos podem conter. Para obter mais informações, consulte Criar documentos recomendados (na página 1021).

Definir marcador em documento

É possível marcar os documentos acessados com frequência. Após um documento ser marcado, ele é adicionado à lista de marcadores. Essa lista pode ajudar a localizar mais rapidamente os documentos que você visualiza com frequência. Após adicionar um documento a uma lista de marcadores, um botão Remover é exibido no campo Marcador. É possível remover os marcadores da lista quando eles não forem mais acessados com frequência.

A pasta Meus indicadores armazena links para os documentos referidos mais freqüentemente. Quando você clica em Meus indicadores no painel Categoria da guia Conhecimento, a lista de documentos com indicadores é exibida no painel Lista de documentos de conhecimento.

Incidentes e problemas

Às vezes, os clientes encontram problemas que não podem ser resolvidos simplesmente ao pesquisar pelo conhecimento. Nem todos os problemas possuem uma solução direta na base de conhecimento. Quando um cliente possui um problema que não pode ser resolvido, ele pode criar um incidente que é enviado para um analista para processamento futuro. O incidente descreve o problema e também pode ser baseado em um documento de conhecimento existente. Quanto mais informação é adicionada ao incidente, mais fácil é para o analista resolver.

Muitas atividades definidas do ITIL são suportadas no Gerenciamento de conhecimento, incluindo as seguintes atividades:

- Gerenciamento de incidentes
  - As pesquisas de conhecimento podem ajudar a encontrar erros conhecidos durante o diagnóstico e investigação futura de incidente
  - Categorização do incidente
- Gerenciamento de problemas
  - Acessar as informações sobre erros conhecidos e ajudar com a correspondência do problema para obter a resolução quando o problema ocorreu anteriormente.
  - Manter e oferecer acesso às informações sobre soluções alternativas.
  - Registrar informações sobre os procedimentos, instruções de trabalho, scripts de diagnóstico e erros conhecidos (enquanto um conteúdo completo, ferramentas de edição, medição e processo de aprovação definível para o desenvolvimento de resoluções)
  - Análise do problema (através da vinculação e análise de incidentes)

Documentos e usuários

A interface de documentos de interface, acessada a partir do nó de Documentos de conhecimento do Gerenciador de filas do CA SDM, permite que todos os usuários do sistema exibam sua Caixa de entrada e comentários de acompanhamento. O administrador gerencia seus documentos não atribuídos/não indexados, políticas automatizadas de ciclo de vida de documentos e fóruns de usuários.

Caixa de entrada de documentos

A Caixa de entrada de documentos de conhecimento (e Caixa de entrada de grupo) no Gerenciador de filas do CA SDM contém documentos atribuídos a você ou ao seu grupo. A caixa de entrada é o repositório central para documentos com todos os status, incluindo documentos de rascunho de retrabalho e de rascunho salvos e atribuídos.

A Caixa de entrada é o recipiente de tarefas diárias está localizado e é uma ferramenta importante pra gerenciar o processo de aprovação. Quando um documento é criado ou atualizado, ele é colocado em uma Caixa de entrada de proprietário. Os itens que aparecem em uma caixa de entrada exigem a atenção do usuário como parte do processo de publicação. Até que sejam publicados, os itens na caixa de entrada não podem aparecer como resoluções e não são adicionados à base de conhecimento. Monitore regularmente sua Caixa de entrada para verificar se há novos documentos.

Exibir comentários de acompanhamento

A Caixa de entrada de comentários de acompanhamento no Gerenciador de filas de documentos de conhecimento do CA SDM contém os comentários atribuídos a você ou ao seu grupo.

É possível exibir informações de resumo para seus comentários de acompanhamento atribuídos na página Lista de comentários.

Para exibir seus comentários de acompanhamento, navegue até Documentos de conhecimento, Comentários de acompanhamento.

Atributos de documento

Definir os atributos do documento ajuda a gerenciar os documentos em seu pool de conhecimento. Os atributos do documento podem ser atualizados para atribuir um novo especialista no assunto ou proprietário do documento. É possível ainda especificar a data em que o documento é disponibilizado na base de conhecimento e a data em que ele expira. Ao selecionar diferentes modelos de documento, é possível modificar a aparência de cada documento.

Permissões do documento

É possível definir, visualizar e editar as permissões para um documento. Essas permissões podem ser atribuídas a diferentes grupos de pessoas. Ao definir as permissões, é possível decidir por herdar as permissões da categoria principal de um documento ou especificar novas permissões. Por padrão, os documentos herdam as permissões de sua categoria principal. Esse padrão trata das permissões de acesso no nível da categoria ao invés de no nível do documento.

Importante: Ao criar um documento de conhecimento, assegure-se de que as permissões do documento incluam usuários que posteriormente possam ser atribuídos no documento pelo processo de aprovação. Quando um grupo é atribuído a um documento, usuários desse grupo podem não ter a permissão de exibir o documento. Se o documento for atribuído a um usuário específico, restrições de partição de dados padrão permitirão que o usuário exiba o documento.

Categorias de conhecimento

Atribua cada documento a uma categoria primária. Por exemplo, qualquer conhecimento relacionado ao Microsoft Word deve ser adicionado à categoria Microsoft Word. Além disso, o Gerenciamento de conhecimento permite associar um documento a várias categorias secundárias e outros documentos. Desta forma, um documento pode ser classificado em muitas categorias diferentes aplicáveis e pode fornecer resultados de pesquisa mais bem sucedidos. Após criar um link de documento, um link *consulte também* é mostrado ao exibir qualquer um dos documentos vinculados. O link *consulte também* permite ir diretamente de um documento vinculado ao outro.

Permissões de anexo

As permissões de anexo são gerenciadas na Biblioteca de anexos, nó de Repositórios na guia Administração É possível definir as permissões da pasta de repositório com base nas necessidades de sua empresa.

Observação: Um documento pode ter diferentes permissões que os anexos vinculados ao documento.

Adicionar um anexo de documento

Ao trabalhar com um documento de conhecimento, você pode vincular arquivos suplementares ou URLs ao documento. Esses arquivos suplementares ou URLs oferecem um acesso fácil às informações relacionadas aos documentos de conhecimento. Os arquivos anexados são armazenados em um repositório.

Use a guia Anexos para gerenciar anexos de arquivo e de URL no documento atual. Em documentos criados usando o modelo padrão Documento de conhecimento interno ou Árvore de documentos de conhecimento interno, os links para anexos são exibidos sob o título "Anexos".

Observação: a guia Anexos é exibida apenas para documentos publicados. Para os documentos não publicados, a guia Anexos exibe as seções Repositórios, Arquivos e Anexos e uma lista de URLs e arquivos atualmente anexados ao documento.

Para adicionar um anexo de arquivo a um documento

1. Abrir o documento para edição.
2. Clique na guia Anexos.
3. Insira o URL que você quer vincular.
4. Proceda de uma das seguintes maneiras:
   - Clique em Anexar arquivo para adicionar um arquivo do seu sistema.
   - Clique em Anexar arquivo da biblioteca para selecionar o nome do arquivo que você quer anexar da lista Repositórios.

   O nome é exibido na guia Anexos.

Exibir o histórico do documento

É possível verificar um registro de todas as ações realizadas em um documento.

Para visualizar o histórico do documento, clique na guia Histórico na página Atualizar documento.

Uma lista de eventos é exibida mostrando os detalhes de cada evento. As informações exibidas na guia Histórico existem para fins de referência a penas e não podem ser modificadas.

Document Notifications (Notificações de documento)

No CA SDM, é possível configurar uma lista de usuários, conhecida como contatos, que podem ser notificados caso determinados eventos ocorram. O processo de notificação informa aos indivíduos sobre a mudança de status de um documento, mantendo-os atualizados ao longo do progresso. Apenas usuários que estejam nessa lista podem receber notificações que foram designadas para um documento.

Mudanças no documento

Após um documento chegar à pasta Caixa de entrada no gerenciador de filas, os usuários podem executar as tarefas atribuídas, modificando e salvando documentos de acordo com suas funções atribuídas (por exemplo, um analista pode ser responsável por verificar o conteúdo técnico do documento, enquanto outro verifica a formatação).

Todos os usuários com permissão completa ao documento podem modificá-lo. O proprietário atual tem permissões completas ao documento, mas não pode ter permissões explícitas de gravação. Apenas o proprietário pode alterar o proprietário do documento (na guia Atributos).

Como gerenciar os privilégios da função e documentar a visibilidade

É possível definir as permissões de segurança do Gerenciamento de conhecimento ao gerenciar os privilégios para os usuários em seu ambiente. Essas permissões fazem com que seja possível definir o que os usuários podem acessar quando desejam visualizar ou criar o conhecimento e como os usuários são autenticados ao efetuarem o logon no sistema.

É possível gerenciar os privilégios de função e a visibilidade dos documentos para Gerenciamento de conhecimento ao realizar as seguintes ações:

1. Na guia Administração, selecione Gerenciamento da segurança e das funções, Gerenciamento de funções, Lista de funções.

   A página Lista de funções aparece.

2. Selecione a função desejada, como Gerente de conhecimento.

   As páginas Detalhes da função e Atualizar função exibem as seguintes guias:

   Gerenciamento de conhecimento

   Especifica os privilégios de Gerenciamento de conhecimento para a função.

   Visibilidade do documento KT

   Especifica quais status do documento a função está autorizada a visualizar, como rascunho, desativado e publicado.

3. Preencha as páginas da guia e salve as mudanças.

   A segurança e os privilégios de função são definidos.

Observação: para obter mais informações sobre a configuração da segurança e a definição de funções, consulte a *Ajuda on-line*.

Action Content

É possível criar "conteúdos de ação" (um URL ao vivo) que pode ser inserido no campo Resolução de um documento de conhecimento que, quando clicado pelo usuário final, cria um incidente ou executa alguma outra ação. Ao usar um conteúdo de ação, pode ser obtido um nível significativo de definição e classificação sem que o usuário mesmo o perceba.

As etapas para inserir um link "conteúdo de ação" em um documento são simples e não é exigida nenhuma codificação. O editor de HTML do Gerenciamento de conhecimento lida com a geração do código HTML .

Observação: conteúdo de ação é principalmente usado para interação com aplicativos externos.

Mais informações:

Exibir conteúdo de ação (na página 958)
Criar conteúdo de ação (URL de ação) (na página 959)
Crie conteúdos de ação (HTMPL Interno) (na página 960)
Editar conteúdo de ação (na página 961)
Pesquisar conteúdo de ação (na página 961)

Exibir conteúdo de ação

É possível exibir os detalhes dos URLs de ação ao vivo que permitem definir ações para os usuários finais. O Gerenciamento de conhecimento permite vincular os documentos de conhecimento com as tarefas automatizadas, então é possível incorporar scripts de autoatendimento nos documentos de conhecimento.

Para exibir o Conteúdo de ação

1. Na guia Administração, navegue até Conhecimento, Conteúdo de ação.

   A Lista de conteúdos de ação aparece.

2. A página exibe os detalhes da ação e as opções de execução.

   Nome

   Exibe o nome do conteúdo da ação.

   Código

   Especifica o código HTML que vincula o conteúdo ao documento.

   URL de ação

   Especifica o link do URL que realiza algum tipo de ação, como a abertura de um website ou um formulário.

   Pesquisar

   Pesquisa itens pelo nome.

   Mostrar filtro

   Pesquisa os itens na página da Lista de comentários. É possível preencher um ou mais campos de pesquisa e clicar em Pesquisar. A página Lista de conteúdo de ação exibe os documentos correspondentes aos critérios.

   Criar novo

   Cria um link de conteúdo de ação.

3. Pesquisa ou conteúdo de ação que pode ser usado com o Gerenciamento de conhecimento e Support Automation.

   Os resultados da pesquisa são exibidos.

Criar conteúdo de ação (URL de ação)

Você pode criar Conteúdo de ação para documentos de conhecimento. Esses URLs de ação podem executar um site ao vivo que seja acessível a todos os usuários de seu sistema. Você pode, também, vincular URLs de ação a tarefas automáticas em seu servidor, e é possível incorporar esses scripts em documentos de conhecimento, documentos da árvore, modelos de documentos e fóruns de conhecimento.

Criar conteúdos de ação (URL de Ação)

1. Na guia Administração, navegue até Conhecimento, Conteúdo de ação.

   A página lista de Conteúdos de ação aparece.

2. Clique em Criar novo.

   A página Criar novo conteúdo de ação é exibida.

3. Preencha os campos. Os campos a seguir precisam de explicação:

   Código

   Especifica um identificador exclusivo para este item de conteúdo de ação.

   Use HTMPL Interno

   Cria um link interno (na página 960)no aplicativo que dinamicamente passa informações, como o nome de usuário e ID de sessão, de documentos de conhecimento para aplicativos de terceiros.. Não selecione esta opção.

   URL de ação

   Especifica um URL que é vinculado a uma página da web, modelo ou script automático, por exemplo: http://www.ca.com.

   Clique em Salvar.

   O conteúdo da ação é criado.

Crie conteúdos de ação (HTMPL Interno)

Você pode criar Conteúdo de ação para documentos de conhecimento. Estes URLs de ação podem executar scripts de autoatendimento e também aplicativos de terceiros. Este link é gerado dinamicamente e transfere automaticamente atributos sobre o usuário, como o nome de usuário, ao aplicativo de destino (http://www.ca.com?USERNAME=BBB, por exemplo). Atributos de usuário são especificados em um arquivo HTMPL.

Para criar um conteúdo de ação com um arquivo HTMPL interno

1. Crie um arquivo HTMPL interno que passe dados ao aplicativo de destino.

   Observação: o arquivo act_content_sample.htmpl está disponível no seguinte local: NX_ROOT\bopcfg\www\htmpl\default.

2. Salve o arquivo HTMPL no seguinte local: NX_ROOT\site\mods\www\htmpl\default directory.

3. A partir da guia Administração, navegue até Conhecimento, Conteúdo de ação.

   A página lista de Conteúdos de ação aparece.

4. Clique em Criar novo.

   A página Criar novo conteúdo de ação é exibida.

5. Preencha o seguinte campo:

   Código

   Especifica um identificador exclusivo para este item de conteúdo de ação.

6. Marque a caixa de seleção HTMPL de Uso Interno.

7. Especifique o arquivo HTMPL apropriado no campo URL de Ação, por exemplo: act_content_sample.htmpl

   Observação: você pode usar scripts do Support Automation usando o formato *SA_SCRIPT=[Self Service Script ID]* no URL.

8. Clique em Salvar.

   O conteúdo da ação é criado. Quando o usuário clicar neste link de Conteúdo de ação dentro de um documento de conhecimento, atributos sobre o usuário, como o nome de usuário, são dinamicamente passados ao aplicativo de destino.

Editar conteúdo de ação

É possível editar conteúdo de ação que já tiver sido criado na página Lista de Conteúdo de ação.

Para editar conteúdo de ação

1. Na guia Administração, selecione Conhecimento, Conteúdo de ação.

   A Lista de conteúdos de ação aparece.

2. Selecione o item que você quer editar.

   A página Detalhe de conteúdo de ação aparece.

3. Clique em Editar.

   A página Atualizar conteúdo de ação aparece.

4. Edite os campos conforme apropriado.
5. Clique em Salvar.

   O conteúdo de ação é atualizado.

Pesquisar conteúdo de ação

Você pode inserir critérios de pesquisa para filtrar a Lista de Conteúdos de ação para exibir somente os itens que você quer ver. Você também pode pesquisar itens individuais para exibir ou editar.

Para pesquisar conteúdo de ação

1. Na guia Administração, selecione Conhecimento, Conteúdo de ação.

   A página Lista de conteúdos de ação é aberta.

2. Clique em Mostrar filtro.

   O filtro Pesquisar aparece.

3. Preencha um ou mais campos de pesquisa:

   Nome

   Identifica este item de conteúdo de ação.

Status

Indica se esse item está Ativo ou Inativo.

Código

Especifica um identificador exclusivo para este item de conteúdo de ação.

Gerenciamento de conhecimento URL

Especifica que o URL de ação é vinculado à página interna da web (.htmpl).

4. (Opcional) Clique em Mais.

   Campos adicionais são exibidos, permitindo que você restrinja ainda mais os itens que aparecem na Lista de conteúdos de ação.

5. Clique em Pesquisar.

   A página Lista de conteúdos de ação exibe os itens correspondentes aos critérios de pesquisa. Você pode selecionar um item para exibir ou editar.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Processo de aprovação de documentos

Para os administradores que desejam controlar o gerenciamento de sua base de conhecimento, a capacidade de personalizar a edição do documento e o processo de aprovação é fundamental. É possível criar modelos do Processo de aprovação que especifica como, quando e por qual funcionário o documento pode ser alterado e publicado para o público. Os modelos do Processo de aprovação podem designar vários processos de aprovação mais adequados para se ambiente de negócios. O processo de aprovação implementado pode ser alterado ao longo do tempo para ser mais simples ou complexo.

O Gerenciador do processo de aprovação permite definir os modelos do Processo de aprovação. Por padrão, o modelo de Processo de aprovação interno é usado. Entretanto, é possível criar um modelo ou editar um existente. Ao criar um modelo de Processo de aprovação, defina os status e adicione tarefas ao modelo. O processo de aprovação envolve diversas tarefas que são realizadas em um documento de conhecimento. O proprietário ao qual um modelo de Processo de aprovação é atribuído realiza cada tarefa.

Os status a seguir são os vários estados ao qual o documento é associado durante os estágios do processo de aprovação:

Rascunho

Especifica um novo documento.

Publicado

Especifica um documento que passou por todo o processo ciclo de aprovação e faz parte da base de conhecimento visualizável.

Versão do Rework-Draft

Especifica uma versão de retrabalho de uma cópia do documento que é substituído na base de conhecimento depois de ser verificado e republicado.

Desativado

Especifica um documento que atingiu sua data de expiração. É possível também criar seus próprios status, que posteriormente são associados às tarefas.

Gerenciador de processo de aprovação

Administradores de conhecimento podem usar o Gerenciador de processo de aprovação para realizar essas ações:

- Determine quais grupos podem ler um documento de conhecimento e quais grupos podem gravar (ou editar) o documento de conhecimento.
- Identifique as tarefas em um modelo de processo de aprovação que determina o ciclo de vida de documentos criados com o modelo.
- Defina os vários status com os quais o documento pode ser associado durante o processo de aprovação.

Importante: Ao criar um documento de conhecimento, assegure-se de que as permissões do documento incluam usuários que posteriormente possam ser atribuídos no documento pelo processo de aprovação. Usuários deste grupo não têm, necessariamente, permissão para visualizar o documento. Se o documento for atribuído a um usuário específico, restrições de partição de dados padrão permitem que o usuário visualize o documento.

Definir um processo de aprovação para a edição de documentos

Administradores de conhecimento podem especificar quem pode editar documentos antes do processo de aprovação e após a publicação.

Observação: usuários com permissões (de leitura/gravação) totais podem editar documentos publicados.

Para definir um processo de aprovação para edição de documentos

1. Na guia Administração, navegue até Conhecimento, Gerenciador de processo de aprovação, Configurações de processo de aprovação.

   A página Configurações de processo de aprovação aparece.

2. Especifique quem pode editar documentos *antes* de sua publicação. Selecione uma das seguintes opções:

   Os documentos podem ser editados por um responsável de tarefa, um proprietário ou por usuários com os modos de exibição de Tipo de acesso apropriados

   Especifica que os seguintes contatos podem editar documentos:

   - Um contato a quem foi atribuída a tarefa atual
   - Um contato especificado como proprietário do documento para a tarefa atual
   - Um gerente de conhecimento
   - Um administrador do sistema

   Os documentos podem ser editados por usuários com permissões totais

   Especifica que qualquer usuário com permissões de gravação possa editar o documento.

3. Especifique quem pode editar documentos *após* sua publicação. Selecione uma das seguintes opções:

   Usuários com permissões totais podem editar documentos após sua publicação

   Especifica que um usuário com permissões totais pode editar documentos publicados.

   Usuários com permissões totais podem alterar atributos de documento publicado

   Especifica que qualquer usuário com permissões de gravação ao documento pode alterar somente atributos de documentos publicados, como itens de configuração ou produtos.

A publicação dos documentos deve ser cancelada para que possam ser editados

Especifica que o usuário deve cancelar a publicação de um documento antes de editá-lo.

Clique em Salvar.

É definido o processo de aprovação.

Criar um modelo de processo de aprovação

As tarefas em um modelo de processo de aprovação definem o ciclo de vida de documentos criados com o modelo.

Observação: se multilocação estiver instalada, selecione o inquilino apropriado na lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos.

Para criar um modelo de processo de aprovação

1. Na guia Administração, selecione Conhecimento, Gerenciador de processo de aprovação, Modelos de processo de aprovação.

   A Lista de modelos de processo de aprovação aparece.

2. Clique em Criar novo.

   A página Detalhes do modelo do processo de aprovação aparece.

3. Insira um nome para o modelo e uma descrição.

4. Clique em Salvar.

   A página Detalhes do modelo de processo de aprovação exibe os campos adicionais.

5. Selecione a tarefa que você quer realizar ao criar uma versão de trabalho do documento, usando este modelo.

6. Selecione a tarefa que você quer realizar ao reativar um documento que foi criado usando este modelo.

7. Clique em Inserir tarefa para criar uma tarefa a ser adicionada ao modelo.

   A página Criar nova tarefa é exibida.

8. Preencha os campos. Os campos a seguir precisam de explicação:

   Tarefa

   Nomeia a tarefa.

Responsável

Atribui uma pessoa à tarefa. Você pode clicar no ícone de pesquisa para selecionar um nome.

Observação: é possível adicionar uma lista alternativa de responsáveis (na página 966) após a tarefa ser criada.

Clique em Salvar.

O modelo de processo de aprovação é criado.

Mais informações:

Adicionar responsáveis alternativos a uma tarefa (na página 966)
Editar um modelo de processo de aprovação (na página 967)
Pesquisar por um modelo de processo de aprovação (na página 967)

Adicionar responsáveis alternativos a uma tarefa

Você pode adicionar responsáveis alternativos ao editar uma tarefa.

Para adicionar responsáveis alternativos a uma tarefa.

1. Selecione a tarefa que você quer editar na lista de Modelo de processo de aprovação.

   A página Detalhes de tarefa aparece.

2. Edite os campos conforme apropriado.
3. Clique no botão Adicionar na Lista de responsáveis.

   A página Criar novo responsável aparece.

4. No campo Responsável, insira o nome da pessoa a quem você quer atribuir à tarefa ou clique no ícone de pesquisa para selecionar o nome.
5. Repita a Etapa 4 conforme necessário para criar uma lista de responsáveis alternativos.
6. Clique em Salvar.

   Os responsáveis alternativos são adicionados à tarefa.

Editar um modelo de processo de aprovação

É possível editar um modelo de processo de aprovação

Para editar um modelo de processo de aprovação

1. Na guia Administração, selecione Conhecimento, Gerenciador de processo de aprovação, Modelos de processo de aprovação.

   A Lista de modelos de processo de aprovação aparece.

2. Selecione o modelo que deseja editar e clique em seu nome.

   A página Detalhes do modelo do processo de aprovação aparece.

3. Clique em Editar.

   A página Atualizar modelo de processo de aprovação aparece.

4. Edite os campos conforme apropriado.
5. Clique em Salvar.

   O modelo de processo de aprovação é atualizado.

Pesquisar por um modelo de processo de aprovação

Você pode inserir critérios de pesquisa para filtrar a Lista de Modelo de processo de aprovação para exibir somente os itens que você quer visualizar. Você também pode pesquisar itens individuais para exibir ou editar.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

Para pesquisar um modelo de processo de aprovação

1. Na guia Administração, selecione Conhecimento, Processo de aprovação, Modelos de processo de aprovação.

   A página Lista de modelos de processo de aprovação aparece.

2. Clique em Mostrar filtro.
3. Digite os primeiros caracteres do nome do modelo que você quer.
4. (Opcional) Clique em Mais.

   Campos adicionais são exibidos, permitindo que você restrinja os itens que aparecem na Lista de modelos de processo de aprovação.

5. Clique em Pesquisar.

   A página Lista de modelos de processo de aprovação exibe os itens correspondentes aos critérios de pesquisa. Você pode selecionar um item para exibir ou editar.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Definições de status de documento

É possível adicionar ou excluir os status de documento definidos pelo usuário e modificar os nomes e descrições dos status de documento predefinidos.

Mais informações:

Criar um status de documento (na página 968)
Pesquisar status de documentos (na página 969)
Editar status do documento (na página 969)

Criar um status de documento

Você pode criar um status de documento para documentos de conhecimento em seu sistema CA SDM.

Para criar um status de documento

1. Na guia Administração, selecione Conhecimento, Gerenciador de processo de aprovação, Status de documento.

   A Lista de status de documento aparece.

2. Clique em Criar novo.

   A página Detalhes do status de documento aparece.

3. Insira um nome e uma descrição para o status.

4. Clique em Salvar.

   O status do documento é criado.

Pesquisar status de documentos

É possível inserir critérios de pesquisa para filtrar a Lista de status do documento para exibir somente os itens que deseja visualizar. Você também pode pesquisar itens individuais para exibir ou editar.

Para pesquisar um status de documento

1. Na guia Administração, selecione Conhecimento, Gerenciador de processo de aprovação, Status de documento.

   A página Lista de status de documento é exibida..

2. Clique em Mostrar filtro.
3. Digite os primeiros caracteres do nome do status que deseja encontrar.
4. (Opcional) Clique em Mais.

   São exibidos campos adicionais, permitindo que você restrinja ainda mais os itens exibidos na Lista de status do documento.

5. Clique em Pesquisar.

   A página Lista status de documentos exibe os documentos correspondentes aos critérios de pesquisa. Você pode selecionar um item para exibir ou editar.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Editar status do documento

É possível editar um status de documento.

Para editar um status de documento

1. Na guia Administração, selecione Conhecimento, Gerenciador de processo de aprovação, Status de documento.

   A Lista de status de documento aparece.

2. Selecione o status que deseja editar e clique sobre seu nome.

   A página Detalhes do status de documento aparece.

3. Clique em Editar.

   A página Atualizar status do documento é exibida.

4. Edite os campos Status e Descrição conforme apropriado.
5. Clique em Salvar.

   O status do documento é atualizado.

Políticas automatizadas

Os administradores podem automatizar determinadas tarefas no processo de aprovação do documento de conhecimento com base nas políticas do ciclo de vida do documento e nas ações que elas definem Ao automatizar as tarefas, os usuários finais procurando por soluções podem resolver os problemas mais rapidamente e também podem fazê-lo sem a necessidade de entrar em contato com outras pessoas, o que representa um benefício para a organização.

As políticas automatizadas funcionam com eventos e macros.

Mais informações:

Exibir políticas automatizadas (na página 970)
Como configurar políticas automatizadas (na página 972)
Criar uma política automatizada (na página 972)
Editar uma política automatizada (na página 973)
Programar políticas automatizadas (na página 974)
Exibir relatórios de política de ciclo de vida de documentos (na página 974)

Exibir políticas automatizadas

Uma política automatizada descreve a condição pela qual documentos são sinalizados para correção e promovidos para publicação ou desativação por vários estágios do processo de ciclo de vida do documento. Por exemplo, você pode especificar a política padrão "corrigir links com problemas" que corresponda aos documentos encontrados na base de conhecimento com links com problemas. A tarefa de corrigir o problema pode ser atribuída a um analista.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

Para exibir políticas automatizadas, selecione a guia Administração, Conhecimento, Políticas automatizadas, Políticas.

A página Lista de políticas automatizadas exibe os detalhes das políticas automatizadas. Você pode editar as políticas padrão ou definir as suas próprias. Cada política está associada aos seguintes componentes:

Consulta armazenada

Contém um conjunto de macros de ação que são executadas quando as políticas identificam e correspondem a um documento durante o processamento. Após o processamento, o evento armazenado de condição de consulta exibe um relatório de política de ciclo de vida do Gerenciamento de conhecimento com base em função no Gerenciador de filas do CA SDM.

O administrador é responsável pelo monitoramento dos relatórios e pelos comentários e recomendações aos editores de documento apropriados.

Macro de ação

Contém código que permite aos usuários definir um sinalizador, aumentar a prioridade ou realizar outras ações. Você pode modificar as macros que aparecem na lista de Macros ou definir as suas próprias.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Mais informações:

Exibir relatórios de política de ciclo de vida de documentos (na página 974)
Programar políticas automatizadas (na página 974)

Como configurar políticas automatizadas

Administradores podem definir o recurso Políticas automatizadas, executando as seguintes etapas:

1. (Obrigatório) Um processamento em lote deve ser definido no Agendador de Políticas Automatizadas que executa no servidor para apresentar os dados necessários para exibir os relatórios de Política de ciclo de vida do Gerenciamento de conhecimento. Essa etapa de ação também se aplica à Ficha de relatório de documento de conhecimento.

   Observação: para obter mais informações sobre políticas automatizadas, consulte o *Guia de implementação*.

2. (Obrigatório) Para gerenciamento da segurança e das funções, defina a etapa pela qual os usuários podem exibir e pesquisar documentos durante seu ciclo de vida na guia Visibilidade do documento de conhecimento em Gerenciamento de funções.

3. Na página Lista de políticas automatizadas, é possível editar as políticas padrão, ou definir as suas próprias.

   Observação: para obter informações sobre novas políticas, o administrador deve incluir o campo "Desconsiderar políticas de ciclo de vida" na consulta armazenada; caso contrário, ela não aparece na guia Atributos.

Criar uma política automatizada

Você pode criar uma política automatizada que é ativada quando uma ação ocorre, como quando um documento é publicado ou desativado da base de conhecimento

Observação: se multilocação estiver instalada, selecione o inquilino apropriado na lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos.

Para criar uma política automatizada

1. Na guia Administração, navegue até Conhecimento, Políticas automatizadas, Políticas.

   A página Criar nova política automatizada é exibida.

2. Digite um nome e descrição para a política nos campos apropriados.
3. Digite um nome de consulta armazenada ou selecione um nome usando o ícone de pesquisa.
4. Clique em Adicionar ação.

   A página Lista de macros aparece.
5. Na página Lista de macros, selecione uma das macros de ação predefinidas, ou defina sua própria (clique em Criar nova).

   A macro de ação aparece na lista de Informações de ação na página Criar nova política automatizada.

   Observação: você pode excluir uma macro de ação: clique com o botão direito do mouse no nome e selecione Excluir no menu de atalho.
6. Clique em Salvar.

   A nova política é exibida na área da lista de políticas automatizadas.
7. (Opcional) Clique com o botão direito do mouse no título para editar uma política.

   A política selecionada aparece na página Atualização de Política e é possível editá-la.

Editar uma política automatizada

Você pode atualizar uma política automatizada.

Para editar uma política automatizada

1. Na guia Administração, navegue até Conhecimento, Políticas automatizadas, Políticas.

   A Lista de políticas automatizadas aparece.
2. Clique com o botão direito do mouse na política a editar e selecione Editar no menu de atalho.

   A página Atualizar política automatizada aparece.
3. Edite os campos de entrada conforme apropriado.
4. Clique em Salvar.

   A política automatizada é atualizada.

Programar políticas automatizadas

É possível especificar a data e a hora em que o CA SDM executa os cálculos e o processamento em lote das políticas.

Para programar políticas automatizadas

1. Selecione a guia Administração, navegue até Conhecimento, Políticas automatizadas, Programando.

   A página Políticas automatizadas aparece.

2. Preencha os seguintes campos:

   Última atualização

   Especifica a caixa de seleção Executar cálculo .

   Cronograma

   Especifica uma data na caixa de texto ou no Calendário. Você pode selecionar o intervalo de tempo em que o CA SDM executa o cálculo e as políticas.

   Clique em Salvar.

   As políticas são processadas na data e horário especificados.

Exibir relatórios de política de ciclo de vida de documentos

Você pode exibir os relatórios de política de ciclo de vida do documento gerados pelas Políticas Automatizadas.

Para exibir os relatórios, selecione a guia Service desk, Documentos de conhecimento, Políticas automatizadas, Políticas.

Quando você seleciona uma política, as seguintes informações de resumo aparecem na página Lista de documentos:

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

Título

Exibe o título do documento que está sinalizado para correção ou promovido para publicação ou desativação.

Política/ações

Exibe o nome da política e conteúdo da ação definida para a política.

Atributos

Exibe as propriedades do documento afetado pela política.

Controle de documento de conhecimento

Quando um usuário abre um documento de conhecimento, é possível adicionar comentários, enviar o conhecimento e visualizar os documentos da árvore de conhecimento. É possível também especificar o conteúdo e a aparência dos documentos ao selecionar um modelo.

Os administradores podem controlar como os usuários interagem com os documentos ao realizar as seguintes tarefas:

- Definir os tipos de comentário (na página 976) que aparecem nos documentos de conhecimento e nas listas suspensas na interface do usuário final.
- Especificar as configurações (na página 1040)do documento relacionadas a comentários, envio de conhecimentos e exibição dos documentos.
- Criar os modelos de documento (na página 982) que especificam o conteúdo e a aparência dos documentos.
- Exportar (na página 925) (ou importar) o conteúdo de conhecimento de outro recurso ou sistema.
- Gerenciar os recursos de controle de versão (na página 909) do documento.
- Gerenciar a Programação dos documentos de conhecimento (na página 913).

Consulte também

Tipos de comentário (na página 976)
Modelos de documentos (na página 982)
Como criar links de documentos de conhecimento (na página 990)

Tipos de comentário

Caso o analista note algum erro de digitação ou problema com o conteúdo de um documento, ele pode adicionar um comentário que sinalizará o documento para correção, atribuindo depois o problema a outro analista para acompanhamento.

Os administradores podem definir os tipos de comentário que aparecem em várias exibições de lista na interface de usuário final.

Exibir os tipos de comentário

Quando um usuário abre um documento de conhecimento, é possível adicionar um comentário que sinalize o documento para correção, promoção ou desativação, e muito mais. A página Lista de tipos de comentário permite gerenciar os detalhes dos tipos de comentário.

Para exibir esta página, selecione a guia Administração, Conhecimento, Documentos, Tipos de comentário.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

A página Lista de tipos de comentário é mostrada e exibe as seguintes colunas:

Nome

Exibe a lista dos tipos de comentário que aparecem nos documentos de conhecimento e nas listas suspensas na interface do usuário. É possível editar definir os tipos de comentário padrão a seguir ou definir o seu próprio:

- Link com problemas
- Candidato para publicação
- Conteúdo não claro
- Difícil de localizar
- Comentário geral

- Informações incorretas
- Informações ausentes
- Recomendar novo conteúdo
- Revisar
- A solução não funciona

Mostrar na exibição de usuários

Mostra o comentário em várias exibições de lista dentro da interface de usuário.

Acompanhamento necessário

Especifica se o usuário é obrigado a responder a este tipo de comentário.

Tempo para conclusão (dias)

Define o número de dias durante o qual o usuário deve acompanhar este tipo de comentário.

Status

Indica se o tipo de comentário está ativo ou inativo.

Essa página contém os seguintes botões:

Pesquisar

Pesquisa itens pelo nome.

Mostrar filtro

Pesquisa um comentário na página da Lista de comentários. Preencha um ou mais campos de pesquisa e clique em Pesquisar. A página Lista de tipos de comentário exibe os comentários correspondentes aos critérios.

Limpar filtro

Limpa o filtro.

Criar novo

Cria um tipo de comentário.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Criar um tipo de comentário

É possível definir os tipos de comentário que aparecem em várias exibições de lista na interface de usuário final na página Criar tipo de comentário.

Observação: se multilocação estiver instalada, selecione o inquilino apropriado na lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos.

Para criar um tipo de comentário

1. Na guia Administração, selecione Conhecimento, Documentos, Tipos de comentário.

   A página Lista de tipos de comentário é exibida.

2. Clique em Criar novo.

   A página Criar tipo de comentário é exibida.

3. Preencha os campos conforme apropriado. Os campos a seguir precisam de explicação:

   Tempo para conclusão (dias)

   Define o número de dias durante o qual o usuário deve acompanhar este tipo de comentário.

   Mostrar na exibição de usuários

   Mostra o comentário em várias exibições de lista dentro da interface de usuário.

   Acompanhamento necessário

   Especifica se o usuário é obrigado a responder a este tipo de comentário.

   Clique em Salvar.

   O novo tipo de comentário aparece na página Lista de tipos de comentário.

Editar um tipo de comentário

É possível atualizar um tipo de comentário que já tenha sido criado na página Lista de tipos de comentário.

Para editar um tipo de comentário

1. Na lista Tipos de comentário, execute uma das seguintes ações:
   - Selecione um comentário e selecione Editar na página Detalhes do tipo de comentário.
   - Clique com o botão direito do mouse em um comentário e selecione Editar no menu de atalho.

   A página Detalhes de tipos de comentário é exibida.
2. Preencha os campos conforme apropriado.
3. Clique em Salvar.

   O tipo de comentário atualizado aparece na página Lista de tipos de comentário.

Document Notifications (Notificações de documento)

No CA SDM, é possível configurar uma lista de usuários, conhecida como contatos, que podem ser notificados caso determinados eventos ocorram. O processo de notificação informa aos indivíduos sobre a mudança de status de um documento, mantendo-os atualizados ao longo do progresso. Apenas usuários que estejam nessa lista podem receber notificações que foram designadas para um documento.

Configurar uma notificação de comentário de acompanhamento

Diversas notificações de atividade padrão listadas na página Lista de notificações de atividade permitem a configuração das notificações para os usuários quando um comentário de acompanhamento for atribuído a eles.

A fila de Comentários de acompanhamento no gerenciador de filas é o repositório para comentários de acompanhamento atribuídos ou não.

Para definir uma notificação de comentário de acompanhamento

1. Na guia Administração, vá para Notificações, Notificações de atividade.

   A página Lista de notificações de atividade aparece.

2. Selecione *uma* das seguintes notificações de atividade:
   - Comentário de acompanhamento atribuído
   - Comentário de acompanhamento fechado

   A página Detalhes da notificação de atividade aparece.
3. Clique em Editar.

   A página Atualizar notificação de atividade aparece.
4. Altere os campos conforme apropriado.
5. Clique em Salvar.

   A página Detalhes da notificação de atividade aparece.
6. Clique em Fechar janela.

   A notificação de atividade modificada aparecerá na Lista de notificações de atividade quando você exibir novamente a lista.

Especificar configurações de documento

Caso você seja um administrador de sistema, é possível especificar as configurações relacionadas aos comentários, ao envio de conhecimento e exibição dos documentos da árvore de conhecimento.

Para especificar configurações do documento

1. Na guia Administração, selecione Conhecimento, Documentos, Configurações do documento.

   A página Configurações do documento é exibida.
2. Preencha os seguintes campos:

   Exibição de documentos da árvore de conhecimento

   Especifica o modo de exibição em que documentos da árvore de conhecimento são abertos. Selecione Abrir em modo Árvore (padrão) para abrir a árvore de documentos de conhecimento diretamente ou Abrir em modo Documento para abrir o documento em exibição de documento. Caso abra no Modo de documento, clique em Exibir para mostrar a árvore de conhecimento.

Comentários

Especifica se os usuários podem enviar comentários para documentos e exibir comentários de documentos. Selecione uma das seguintes opções:

- **Permitir envio e exibição de comentários (padrão)**—Exibe um campo de Comentário na parte inferior do documento aberto para que os usuários possam enviar comentários para o documento. Os usuários podem exibir comentários já associados com o documento aberto.
- **Permitir envio de comentários, mas não exibição**—Exibe um campo de Comentário na parte direita de um documento aberto para que os usuários possam enviar comentários para o documento. Os usuários não podem exibir comentários já associados com o documento aberto.
- **Não permitir envio nem exibição de comentários**—Nega aos usuários a capacidade de enviar ou exibir comentários. O campo Comentário não é exibido em um documento aberto.

Enviar conhecimento

Define o repositório para os documentos enviados pelo usuário. O produto preenche a lista com os nomes dos repositórios definidos no painel Biblioteca de anexos.

considere as seguintes informações:

- Quando um analista cria um documento na categoria que tem um proprietário e atribui o documento ao proprietário da categoria:

  O proprietário da categoria se tornará o destinatário e o proprietário do documento.

  O proprietário da categoria deverá receber uma notificação de documento atribuído.

- Quando um analista cria um documento na categoria que não tem um proprietário e atribui o documento ao proprietário da categoria:

  Ninguém se torna o responsável ou proprietário do documento.

  Enviar notificação deve enviar o documento de conhecimento, conforme definido na administração.

- Quando um analista cria um documento e atribui o documento ao proprietário da categoria:

  Esse usuário é responsável e proprietário.

  A notificação não é enviada.

- Quando um funcionário ou cliente cria novos documentos, o CA SDM executa a ação como declarada nos primeiros dois pontos.

Tamanho máximo de resolução

Define o tamanho máximo (em caracteres) que o campo Resolução em um documento pode conter.

Limites: O número máximo permitido de caracteres é 256000.

Padrão: 32768

Anulação de documentos duplicados

Força a pesquisa por documentos semelhantes quando o usuário cria um documento de conhecimento.

Notificação antes da expiração

Define o número de dias antes da expiração do documento e envia uma notificação.

Padrão: 7

Observação: esse valor só se aplica a documentos atualizados ou criados no CA SDM. Se os documentos forem migrados do CA SDM r11.2 e as datas de expiração estiverem definidas para antes da migração, essa opção não se aplica a menos que, ou até que, os documentos sejam atualizados após a migração.

Clique em Salvar.

As mudanças são aplicadas ao abrir um documento de conhecimento ou um documento da árvore de conhecimento.

Modelos de documentos

É possível usar os modelos de documento para controlar o formato e o conteúdo padrão dos documentos de conhecimento. Todos os documentos de conhecimento usam um modelo de documento para definir suas propriedades e aparência quando abertos. Por padrão, um modelo interno está associado com novos documentos de conhecimento.

O Editor de modelo permite fazer o seguinte:

- Projetar um modelo de documento que pode ser posteriormente associado a um documento na guia Conteúdos da página Editor de documento.
- Modificar o modelo interno e outros modelos.

  Ao editar os modelos, é possível criar modelos para associar aos documentos. É possível selecionar as opções de Propriedade e editar as seções Cabeçalho e Corpo usando o Editor de HTML.
- Atualizar os modelos de documento a partir de uma release anterior para suportar os relacionamentos de conhecimento (na página 989), como links pai-filho.

Criar um modelo de documento

Um modelo de documento especifica o conteúdo e a aparência dos documentos na base de conhecimento. É possível aplicar os modelos padrão:

- Interno - Documento de conhecimento
- Interno - Documento da árvore de conhecimento
- Interno - Edição rápida

O produto usa os modelos padrão quando cria documentos de conhecimento e documentos da árvore de conhecimento, a menos que você crie modelos de documento e os associe com seus documentos.

Observação: ao criar um documento de conhecimento, selecione o inquilino adequado para a lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos.

Para criar um modelo de documento

1. Na guia Administração, navegue até Conhecimento, Documentos, Modelos de documento.

   A página Lista de modelos de documento é exibida.
2. Clique em Criar novo.

   A página Criar modelo de documento é exibida.
3. Preencha os seguintes campos:

   Modelo

   (Obrigatório) Define um nome exclusivo para o modelo.

Detalhes

Exibe o conteúdo estático que é exibido em documentos criados usando-se o modelo atual. Se selecionar a opção Código-fonte HTML, você poderá editar código HTML para o corpo diretamente no Corpo. Se selecionar a opção Exibição rápida, o campo Corpo será somente leitura e exibirá o conteúdo estático do corpo como ele é exibido no tempo de execução.

4. (Opcional) Clique em Definir valores do padrão.

   A página Modelo de valores padrão é exibida.

   É possível definir os valores padrão ao criar um documento. Caso um modelo seja alterado em um documento existente, não há impacto.

5. (Opcional) Oculte o Título, Resumo, Problema ou Resolução de seu modelo.

   É possível ocultar esses campos quando desejar um documento simples, como um modelo de perguntas e respostas.

6. Clique em Editar Detalhes.

   A página do Editor de HTML é exibido e é possível especificar o conteúdo estático e o layout de documentos que usam o modelo. É possível editar o código usando a barra de ferramentas para inserir marcas de espaço reservado.

   Importante: É possível remover os relacionamentos de conhecimento, como pai, filho e links relacionados, ao excluir as marcas {TAG_PARENT} e {TAG_RELATED} do modelo.

7. Clique em OK.

   O campo Detalhe mostra o conteúdo atualizado.

8. (Opcional) Clique em Exibição rápida.

   Exibe o conteúdo assim como ele aparece nos documentos com base no modelo.

9. (Opcional) Clique em Exibição HTML.

   Exibe o conteúdo como código HTML.

10. Clique em Salvar.

    A página Detalhes do modelo de documento aparece.

11. Clique em Fechar janela.

    Novos documentos que usam o modelo mostram o novo conteúdo e layout.

    O nome do modelo é exibido na Lista de modelo ao exibir a lista novamente.

Observação: as mudanças realizadas no documento usando o modelo são exibidas após iniciar uma nova sessão ao efetuar o logon no sistema.

Editar um modelo de documento

É possível editar o nome, o layout e o conteúdo de um modelo usando o Gerenciamento de conhecimento.

Para atualizar um modelo de documento

1. Na guia Administração, navegue até Conhecimento, Documentos, Modelos de documento.

   A seção Lista de modelos de documento é exibida.

2. Selecione um nome de modelo.

   A página Atualizar modelo de documento aparece.

3. Clique em Editar Detalhes.

   O Editor de HTML é aberto.

4. Altere o nome, o conteúdo ou o layout do modelo. É possível alterar os seguintes campos:

   Modelo

   Define um nome exclusivo para o modelo. Esse campo é obrigatório.

   Detalhes

   Exibe o conteúdo estático que é exibido em documentos criados usando-se o modelo atual. Se selecionar a opção Código-fonte HTML, você poderá editar código HTML para o corpo diretamente não campo Corpo. Se selecionar a opção Exibição rápida, o campo Corpo será somente leitura e exibirá o conteúdo estático do corpo como ele é exibido no tempo de execução.

5. Clique em Editar detalhes para especificar o conteúdo estático e o layout dos documentos que usam o modelo.

   A janela do Editor de HTML é aberta.

6. Edite o código usando a barra de ferramentas para inserir marcas de espaço reservado. Clique em OK.

   O campo Detalhe mostra o conteúdo atualizado.

7. (Opcional) Clique em Exibição rápida.

   O conteúdo é exibido como um documento com base no modelo.

8. (Opcional) Clique em Exibição HTML.

   O conteúdo é exibido como código HTML.

9. Clique em Salvar.

   A página Detalhes do modelo de documento aparece.

10. Clique em Fechar janela.

    Novos documentos que usam o modelo mostram o novo conteúdo e layout.

    Uma mudança do nome do modelo é exibida na lista quando ela é atualizada.

Relacionar modelos de documento

Use a página Lista de modelos de documento para criar e gerenciar modelos de documento, que especificam o conteúdo e a aparência de documentos na base de conhecimento.

Os modelos padrão a seguir são instalados com o produto:

- Interno - Documento de conhecimento
- Interno - Documento da árvore de conhecimento
- Interno - Edição rápida

O produto usa os modelos padrão quando cria documentos de conhecimento e documentos da árvore de conhecimento, a menos que você crie modelos de documento e os associe com seus documentos.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

Para listar modelos de documento, selecione Administração, Conhecimento, Documentos, Modelos de documento na guia Administração.

A página Lista de modelos do documento é mostrada e inclui as seguintes colunas:

Nome do modelo

Lista os modelos de documento atualmente definidos no produto. Selecione um nome de modelo para abrir a janela Atualizar modelo de documento. Clique com o botão direito do mouse em um nome de modelo para abrir o menu de atalho Nome do modelo, que contém comandos para trabalhar com o modelo selecionado.

Padrão

Exibe uma marca para indicar que um modelo é usado por padrão para novos documentos ou quando o modelo especificado para um documento é excluído. É possível definir um modelo como o padrão, ao clicar com o botão direito do mouse no nome do modelo e selecionar Definir como padrão no menu de atalho.

Observação: quando criar um documento ou excluir um modelo associado a um documento, o produto associa o modelo padrão com ele (a menos que especifique outro modelo na guia Atributos da janela Criar novo documento ou na janela Atualizar documento de conhecimento).

Essa página contém os seguintes campos:

Modelo

Define o nome do modelo pelo qual se deve pesquisar. Esse campo só é exibido quando você clica em Mostrar filtro.

Argumentos de pesquisa adicionais

Define os critérios adicionais pelos quais se deve pesquisar. Esse campo só é exibido quando você clica no link Mais no painel Pesquisa de conhecimento.

Essa página contém os seguintes botões:

Limpar filtro

Retorna todos os campos de filtro no painel ou janela a seus valores padrão.

Criar novo

Abre a janela Criar novo modelo de documento para que você possa definir um novo modelo de documento.

Pesquisar

Inicia uma pesquisa por itens que correspondam aos critérios especificados. Quando você não especifica nenhum critério, o produto retorna todos os itens apropriados (por exemplo, pastas/documentos, contatos, modelos, palavras não pesquisáveis ou grupos de permissões).

Mostrar/Ocultar filtro

Exibe ou oculta campos com os quais você pode filtrar uma pesquisa por itens na janela, painel ou caixa de diálogo atual.

Observação: os usuários podem exportar os resultados das listas para Excel a fim de usá-las fora do CA SDM clicando no botão Exportar na página Lista.

Filtrar a lista de modelos de documento

Os modelos padrão são usados quando documentos de conhecimento e documentos da árvore de conhecimento são criados, a menos que você crie modelos de documento e os associe com seus documentos. Use a página Lista de modelos de documento para criar e gerenciar modelos de documento, que especificam o conteúdo e a aparência de documentos na base de conhecimento. É possível filtrar os modelos a partir dessa página.

Para filtrar a lista de modelos de documento

1. Clique na guia Administração.

   A página Administração aparece.

2. Clique em Conhecimento, Documentos, Modelos de documento.

   A Lista de modelos de documento é exibida.

3. Proceda de *uma* das seguintes maneiras:

   - Selecione um modelo da coluna Nome do modelo.

     O Modelo é aberto.

   - Procure por um modelo usando essa função.

     Os resultados da pesquisa de modelos são exibidos.

   - Selecione Mostrar filtro para filtrar sua pesquisa.

     A pesquisa do modelo é filtrada.

Atualize os modelos de documento para exibir os links de relacionamento de conhecimento

É possível atualizar os modelos de documentos de conhecimento a partir de uma release anterior do CA SDM para exibir os relacionamentos de conhecimento. Modifique o modelo ao adicionar as marcas {TAG_PARENT} e {TAG_RELATED}, permitindo que os documentos usando o modelo exibam os relacionamentos do documento, como pai-filho e inquilino.

Para modificar os modelos para exibirem relacionamentos de conhecimento

1. Abra o modelo de documento de conhecimento.

   A página Atualizar modelo de documento aparece.

2. Clique em Editar.

3. Selecione a exibição do código-fonte HTML.

   Observação: é possível também clicar em Editar detalhes, abrir o Editor de HTML e adicionar as marcas {TAG_PARENT} e {TAG_RELATED}.

4. Selecione *Selecionar espaço reservado para o modelo* na lista suspensa Editar detalhes para adicionar as marcas ao modelo do documento.

   As marcas são adicionadas ao modelo.

5. Salve e feche o modelo.

   O modelo é atualizado para exibir os relacionamentos de conhecimento.

Como criar links de documentos de conhecimento

É possível manter seu ambiente Gerenciamento de conhecimento ao criar links de documento. Os relacionamentos de conhecimento permitem a criação de hierarquias de documentos e o gerenciamento de mudanças para seus documentos de conhecimento.

É possível criar os relacionamentos de conhecimento da seguinte maneira:

1. Configure os modelos de documento de conhecimento para exibir ou ocultar os relacionamentos pai-filho no modo de exibição.
2. Crie ou modifique um documento de conhecimento.

   Observação: por padrão, é possível apenas adicionar links a um documento de conhecimento não publicado. Se o documento já tiver sido publicado, abra o documento no modo de edição ou retrabalho para criar links de documento. É possível modificar as permissões para documentos antes do processo de aprovação e após a publicação.
3. Crie *qualquer* um dos links de documentos a seguir a partir da guia Conhecimento relacionado, conforme for adequado para seu ambiente do Gerenciamento de conhecimento:
   - Vincule o documento como um Consulte também não hierárquico.

     É possível vincular os documentos de conhecimento a outros documentos existentes.
   - Vincule o documento como um pai ou filho.

     É possível criar um link para documentos de conhecimento em relacionamentos pai-filho.

     Observação: caso modifique um documento pai, é exibido um alerta dizendo que os documentos filho podem ser afetados.
   - Vincule o documento global como um documento de inquilino.

     É possível vincular os documentos de conhecimento a um único inquilino ou a vários inquilinos. Por exemplo, um documento filho pode ter um inquilino diferente do documento pai.

   A guia Histórico é atualizada ao criar links de documento para ajudar a acompanhar as mudanças.
4. Salve o documento e verifique se o link é exibido ao abrir o documento na Exibição do usuário.

   É possível verificar se os links de documento são exibidos de acordo com as permissões estabelecidas.

Criar um link de Pai-filho

É possível criar relacionamentos de pai-filho para documentos de conhecimento. Use os links de pai-filho para organizar os documentos relacionados para os usuários em seu ambiente.

Para criar um link de pai-filho

1. Crie um documento de conhecimento ou abra um documento no modo de edição.

   O documento de conhecimento aparece.

2. Selecione a guia Conhecimento relacionado.

   A página Categorias aparece.

   Observação: É possível também criar links na guia Localizar item semelhante. Use os critérios de pesquisa para localizar os documentos.

3. Localize o documento que deseja vincular na seção Categorias (X).

   Clique com o botão direito do mouse na seção Documentos e selecione a opção *Link this as Parent* ou *Link this as Child* para criar o link entre os documentos.

   O link de documento é criado.

Criar um link Consulte também

É possível criar um relacionamento Consulte também para documentos de conhecimento em seu ambiente. Use os relacionamentos Consulte também para gerenciar as hierarquias de conhecimento em seu ambiente.

Para criar um link Consulte também

1. Crie um documento de conhecimento ou abra um documento no modo de retrabalho.

   O documento de conhecimento aparece.

2. Selecione a guia Conhecimento relacionado.

   A página Categorias aparece.

   Observação: É possível também criar links na guia Localizar item semelhante.

3. Localize o documento que deseja vincular na seção Categorias (X).

   Clique com o botão direito do mouse no documento na seção Documentos e selecione a opção *Vincular este documento como Veja também*.

   O link de documento é criado.

Removendo links de documento

É possível remover os links de um documento de conhecimento não publicado, como um relacionamento de pai-filho. Se o documento já tiver sido publicado, abra o documento no modo de edição ou retrabalho para remover links de documento.

Para remover um link de documento,

1. Abra o documento de conhecimento.

   O documento é exibido.

2. Clique em Editar.

   A página Atualizar documento aparece.

3. Selecione a guia Conhecimento relacionado.

   A página Categorias aparece.

4. Navegue até a seção Links de documento.

5. Selecione a opção *Remover este link* no menu de contexto para remover o link.

   Os links do documento são removidos.

Categorias de conhecimento

Os documentos de conhecimento estão organizados em *categorias de conhecimento*. Os engenheiros de conhecimento, gerentes de conhecimento e administradores podem gerenciar as categorias. Cada um desses indivíduos usa o Gerenciamento de conhecimento para criar, copiar e modificar as categorias. Porém, apenas os gerentes de conhecimento e administradores podem excluir categorias. Ao criar a estrutura da categoria em Categorias de conhecimento, você cria a estrutura hierárquica que os funcionários do service desk, clientes e analistas usam para navegar para documentos relevantes.

Atribua cada documento a uma categoria primária. Por exemplo, qualquer conhecimento relacionado ao Microsoft Word deve ser adicionado à categoria Microsoft Word. Além disso, o Gerenciamento de conhecimento permite associar um documento a várias categorias secundárias e outros documentos. Desta forma, um documento pode ser classificado em muitas categorias diferentes aplicáveis e pode fornecer resultados de pesquisa mais bem sucedidos.

A estrutura da categoria realiza as seguintes funções:

- Organiza as soluções de conhecimento em grupos gerenciáveis.
- Faz com que seja mais fácil atribuir os direitos de acesso.
- Faz com que seja possível pesquisar as soluções usando o FAQ/Procura.

  Para usar a funcionalidade de procurar a categoria de um incidente, a área de incidente e a categoria de conhecimento devem corresponder. Ao criar um incidente com base em um documento de conhecimento, a categoria do documento define a área do incidente, assim a categoria e a área sempre correspondem.
- Cria um link de documento - Um link *consulte também* é mostrado ao exibir qualquer um dos documentos vinculados. O link *consulte também* permite ir diretamente de um documento vinculado ao outro.

Criar uma categoria de conhecimento

Para cada categoria, você pode definir propriedades que identificam atributos ou qualidades a serem associadas ao ticket e criar um fluxo de trabalho que identifique todas as tarefas individuais necessárias para concluir o ticket.

Você pode usar categorias para especificar valores padrão para determinados campos nos tickets ou automaticamente associar um nível de serviço a tickets atribuindo um tipo de serviço padrão às categorias. Sempre que um analista atribui uma categoria a um ticket, todas as informações que você associa à categoria são automaticamente associadas ao ticket.

Observação: se estiver usando multilocação, uma lista suspensa de inquilino é exibida no filtro de pesquisa Documento de conhecimento. Se você selecionar <vazio> nessa lista suspensa, a pesquisa será pública. Uma coluna de inquilinos também aparecerá na página da lista.

Para criar uma categoria

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse na categoria sob a qual deseja criar a categoria. Selecione Nova categoria no menu de atalho.

   A página Criar categoria é aberta na guia Conteúdo.

3. Preencha os campos (na página 996) conforme apropriado.

4. Clique em Permissões.

   A guia Permissões é exibida.

5. Selecione uma das seguintes opções de permissão para a categoria:

   Herdar de pai

   Especifica que a nova categoria tem as mesmas configurações de permissão que sua categoria pai.

   Observação: a opção Herdar de pai não está disponível se for selecionada a categoria TOP antes de abrir a página Create Category.

Controle por grupo

Especifica permissões de categoria para que os grupos tenham acesso de leitura ou gravação à categoria.

Controle por função

Especifica permissões de categoria para que as funções tenham acesso de leitura ou gravação à categoria.

Observação: se os controles forem alterados, por exemplo, ao alterar a permissão de categoria de grupo para função, é exibido um aviso de que as permissões anteriores serão excluídas para aquela categoria.

Conceder permissão de gravação a todos

Especifica que todos os usuários têm acesso de gravação à categoria. O acesso de gravação indica que é possível editar ou excluir essa categoria.

Observação: a caixa de seleção Conceder permissões de leitura a todos será automaticamente selecionada se você selecionar a caixa de seleção Conceder permissões de gravação a todos.

Conceder permissão de leitura a todos

Especifica que todos os usuários têm acesso de leitura à categoria. A permissão de leitura indica que é possível visualizar a categoria, mas não pode editar ou excluí-la. Os usuários com direitos administrativos podem editar uma pasta ainda que seu grupo de permissões associado não possa. Se um usuário pertencer a vários grupos de permissão com níveis variáveis de acesso à categoria, o usuário obtém o mais alto nível de acesso disponível (por exemplo, se um grupo tiver acesso apenas de leitura e o outro acesso de gravação, o usuário obtém acesso de gravação).

Observação: a caixa de seleção Conceder permissões de leitura a todos será automaticamente selecionada se você selecionar a caixa de seleção Conceder permissões de gravação a todos.

Importante: ao conceder permissão para Todos, o acesso por função ou grupo é o mesmo. Se você selecionou Todos e Controle por função, após salvar as permissões, o Controle por grupo fica selecionado.

6. (Opcional) Especifique as permissões de leitura e gravação para funções ou grupos específicos nas listas Disponível e Selecionado.

Você usa esta opção para gerenciar quais grupos ou funções possuem acesso de leitura ou gravação na categoria. É possível selecionar um ou mais funções ou grupos de permissão da lista Grupos/Funções disponíveis, e em seguida usar os botões Adicionar e Remover para mover os grupos ou funções selecionados para as listas Groups/Roles with Write Permission e Groups/Roles with Read Permission.

7. Clique em Salvar.

   A página Detalhes da categoria aparece.

8. Clique em Fechar janela.

   A seção Categorias de conhecimento é atualizada para incluir a nova categoria.

Mais informações:

Campos da categoria (na página 996)

Campos da categoria

Título

Nomeia a categoria.

Descrição

Descreve a categoria.

Proprietário da categoria

Indica a pessoa responsável pela categoria. Quando um contato é definido como o proprietário de uma categoria, ele terá um link na Ficha de relatório de documento de conhecimento denominado “Minhas categorias”, a partir do qual ele poderá exibir as estatísticas para aquela categoria e os documentos que ela contém. Esta pessoa é também a proprietária padrão para novos documentos na categoria quando o usuário que cria os documentos não é um analista, ou um analista que crie os documentos com a opção 'Atribuir ao proprietário da categoria' selecionada.

Modelo de documentos

Define o modelo de documento a ser usado para todos os documentos associados a essa categoria. A opção <vazio> significa que nenhum foi definido, mas que, por padrão, o modelo predefinido é usado.

Modelo do processo de aprovação

Define o modelo padrão a ser usado para o processo de aprovação de todos os documentos associados a essa categoria. O modelo de processo de aprovação define as etapas do fluxo de trabalho que um documento deve percorrer antes de ser publicado. O padrão é <vazio>, o que indica que o modelo padrão de aplicativo é usado.

Permite que fóruns sejam criados nesta categoria

Especifica se o analista pode criar fóruns nessa categoria.

Área de solicitação/incidente/problema

Designa uma Área de solicitação/incidente/problema que seu administrador define para designar uma área de responsabilidade. Você pode clicar no ícone de pesquisa para selecionar dentre as áreas disponíveis.

Categoria da ocorrência

Designa uma Categoria de ocorrência que seu administrador define para designar uma área de responsabilidade. Você pode clicar no ícone de pesquisa para selecionar dentre as áreas disponíveis.

Modificar uma categoria

É possível modificar uma categoria em seu ambiente Gerenciamento de conhecimento. As categorias determinam o conteúdo de requisições de mudança e ocorrências depois da sua criação. Para cada categoria, você pode definir propriedades que identificam atributos ou qualidades a serem associadas ao ticket e criar um fluxo de trabalho que identifique todas as tarefas individuais necessárias para concluir o ticket.

Você pode usar categorias para especificar valores padrão para determinados campos nos tickets ou automaticamente associar um nível de serviço a tickets atribuindo um tipo de serviço padrão às categorias. Sempre que um analista atribui uma categoria a um ticket, todas as informações que você associa à categoria são automaticamente associadas ao ticket.

Para modificar uma categoria

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse no arquivo a ser modificado e selecione Editar categoria do menu de atalho.

   A página Atualizar categoria é aberta na guia Conteúdo.

   Observação: não é possível excluir nem modificar a categoria Topo

3. Atualize um ou mais campos (na página 996) adequadamente

4. Clique em Permissões.

   A guia Permissões é exibida.

5. Selecione uma das seguintes opções de permissão para a categoria:

   Herdar de pai

   Especifica que a nova categoria tem as mesmas configurações de permissão que sua categoria pai.

   Observação: a opção Herdar de pai não está disponível se for selecionada a categoria TOP antes de abrir a página Create Category.

   Controle por grupo

   Especifica permissões de categoria para que os grupos tenham acesso de leitura ou gravação à categoria.

   Controle por função

   Especifica permissões de categoria para que as funções tenham acesso de leitura ou gravação à categoria. Se você selecionou Todos e Controle por função, após salvar as permissões, o Controle por grupos fica selecionado.

   Observação: se os controles forem alterados, por exemplo, ao alterar a permissão de categoria de grupo para função, é exibido um aviso de que as permissões anteriores serão excluídas para aquela categoria.

6. (Opcional) Especifique as permissões de leitura e gravação para a categoria.

   Você usa esta opção para gerenciar quais grupos ou funções possuem acesso de leitura ou gravação na categoria. Ao selecionar essa opção, a página é atualizada para incluir as caixas de opção (na página 1002) Conceder permissão de gravação a todos e Conceder permissão de leitura a todos.

7. Clique em Salvar.

   A categoria modificada é exibida na página Knowledge Categories List.

Excluir uma categoria

É possível remover uma categoria da estrutura de Categoria do documento de conhecimento. Ao excluir uma categoria, é possível especificar se as subcategorias e todos os links de documentos associados devem ser removidos

Observação: Este recurso está disponível somente para administradores do sistema e gerentes de conhecimento.

Para excluir uma categoria

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse no arquivo a ser excluído e selecione Excluir categoria do menu de atalho.

   A página Excluir categoria é exibida.

   Observação: não é possível excluir nem modificar a categoria Topo

3. (Opcional) Proceda de *uma* das seguintes maneiras:

   - Marque a caixa de seleção Incluir subcategorias para excluir todas as subcategorias da categoria selecionada.
   - Desmarque a caixa de seleção Incluir subcategorias para mover todas as subcategorias da categoria selecionada para a categoria pai mais próxima que estiver disponível.

4. (Opcional) Proceda de *uma* das seguintes maneiras:

   - Marque a caixa de seleção Incluir documentos para excluir documentos que residem na categoria selecionada. Ao marcar a caixa de seleção Incluir documentos, as seguintes opções são exibidas:
     - **Excluir os documentos vinculados apenas por categoria primária** — Exclui apenas documentos cuja categoria selecionada esteja identificada na seção Categorias de conhecimento como a categoria primária do documento.

- **Excluir todos os documentos vinculados à categoria** — Exclui todos os documentos na categoria selecionada.

■ Selecione a caixa de seleção Incluir documentos para realocar documentos da categoria selecionada para a categoria pai mais próxima que estiver disponível.

Clique em OK.

O produto exclui a categoria selecionada e a seção de Categoria do documento de conhecimento é atualizada.

Mover uma categoria

É possível mover uma categoria, suas subcategorias e todos os links de documento associados de sua localização atual para outra categoria.

Observação: esse recurso está disponível apenas quando o Gerenciamento de conhecimento está instalado.

Para recortar e colar uma categoria

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse no arquivo a ser movido e selecione Recortar categoria do menu de atalho.

   O produto armazena na memória a categoria selecionada, suas subcategorias e todos os links de documentos associados.

3. Clique com o botão direito do mouse na categoria em que deseja colar as informações recortadas e selecione Colar categoria no menu de atalho.

   A categoria recortada é movida de sua localização original para abaixo da categoria selecionada. A seção Categorias de conhecimento é atualizada para mostrar a nova estrutura de categoria.

Copiar uma categoria com links de documento

É possível colocar uma cópia de uma categoria, suas subcategorias e todos os links de documentos associados em outra categoria sem remover a seleção de seu local original.

Para copiar e colar uma categoria com os links de documento

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse no arquivo a ser copiado e selecione Copiar categoria com links de documento do menu de atalho.

   O produto armazena na memória a categoria selecionada, suas subcategorias e todos os links de documentos associados.

3. Clique com o botão direito do mouse na categoria na qual colar as informações copiadas e em seguida selecione Colar categoria no menu de atalho.

   As informações copiadas aparecem abaixo da categoria selecionada. A seção Categorias de conhecimento é atualizada para mostrar a nova estrutura de categoria.

Copiar uma categoria sem links de documento

É possível colocar uma cópia de uma categoria e suas subcategorias sem remover a seleção de seu local original ou copiar os links de documentos associados.

Para copiar e colar uma categoria sem links de documento

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse no arquivo a ser copiado e selecione Copiar categoria do menu de atalho.

   O produto armazena a categoria selecionada e suas subcategorias na memória.

3. Clique com o botão direito do mouse na categoria na qual colar as informações copiadas e em seguida selecione Colar categoria no menu de atalho.

   As informações copiadas aparecem abaixo da categoria selecionada. A seção Categorias de conhecimento é atualizada para mostrar a nova estrutura de categoria.

Gerenciar permissões de categoria

É possível gerenciar permissões de categoria em seu ambiente Gerenciamento de conhecimento, concedendo permissões específicas de leitura/gravação com base no grupo ou função. É possível especificar quem pode visualizar, editar, excluir ou adicionar subcategorias a uma categoria.

Observação: você pode usar permissões de gravação vazias para documentos e categorias . São definidas permissões de gravação vazias quando você não seleciona permissões de gravação. Apenas usuários privilegiados podem modificar categorias e documentos com permissões de gravação vazias.

Para gerenciar permissões de categoria

1. Na guia Administração, navegue até Conhecimento, Categorias de conhecimento.

   A página Categorias de conhecimento é exibida.

2. Clique com o botão direito do mouse na categoria sob a qual você quer criar a categoria, e selecione Nova categoria no menu de atalho para gerenciar as permissões de uma nova categoria .

   A página Criar categoria exibe a guia Conteúdo.

3. Clique em Permissões.

   A guia Permissões é exibida.

4. Selecione uma das seguintes opções de permissão para a categoria:

   Herdar de pai

   Especifica que a nova categoria tem as mesmas configurações de permissão que sua categoria pai.

   Observação: se você selecionar a categoria Principal antes de abrir a página Criar nova categoria, a opção Herdar do Pai não fica disponível.

Controle por grupo

Especifica permissões de categoria para que os grupos tenham acesso de leitura ou gravação à categoria.

Controle por função

Especifica permissões de categoria para que as funções tenham acesso de leitura ou gravação à categoria.

Observação: se você alterar os controles, como, por exemplo, definir a permissão do grupo até a função, é exibido um aviso que diz que as permissões existentes estão excluídas.

Conceder permissão de gravação a todos

Especifica que todos os usuários têm acesso de gravação à categoria. O acesso de gravação indica que é possível editar ou excluir essa categoria.

Observação: a caixa de seleção Conceder permissões de leitura a todos será automaticamente selecionada se você selecionar a caixa de seleção Conceder permissões de gravação a todos.

Conceder permissão de leitura a todos

Especifica que todos os usuários têm acesso de leitura à categoria. A permissão de leitura indica que é possível visualizar a categoria, mas não pode editar ou excluí-la. Os usuários com direitos administrativos podem editar uma pasta ainda que seu grupo de permissões associado não possa. Se um usuário pertencer a vários grupos de permissão com níveis variáveis de acesso à categoria, o usuário obtém o mais alto nível de acesso disponível (por exemplo, se um grupo tiver acesso apenas de leitura e o outro acesso de gravação, o usuário obtém acesso de gravação).

Observação: a caixa de seleção Conceder permissões de leitura a todos será automaticamente selecionada se você selecionar a caixa de seleção Conceder permissões de gravação a todos.

Importante: ao conceder permissão para Todos, o acesso por função ou grupo é o mesmo. Se você selecionou Todos e Controle por função, após salvar as permissões, o Controle por grupo fica selecionado.

5. Conceda as permissões apropriadas de leitura/gravação a grupos ou funções específicos das listas Disponíveis e Selecionadas.

   É possível selecionar um ou mais funções ou grupos de permissão da lista Grupos/Funções disponíveis, e em seguida usar os botões Adicionar e Remover para mover os grupos ou funções selecionados para as listas Groups/Roles with Write Permission e Groups/Roles with Read Permission.

   Observação: todos os grupos ou funções adicionados à lista de permissão são automaticamente adicionados à lista de permissão de leitura. Ao selecionar a caixa de seleção Conceder permissão de Leitura a Todos, não é necessário adicionar grupos ou funções à lista de permissão de leitura..

6. Clique em Salvar.

   A página Detalhes da categoria aparece.

7. Clique em Fechar janela.

   A categoria modificada é exibida na seção Categorias de conhecimento.

Relatórios e métricas

É possível monitorar a eficiência da base de conhecimento usando as seguintes ferramentas de relatório:

- Ficha de relatório de conhecimento
- Relatórios com base na web para o Gerenciamento de conhecimento
- Formulários da Web com base em função

Estas ferramentas permitem exibir as estatísticas sobre a utilidade de seus documentos e sua efetividade na solução de problemas.

Mais informações:

Ficha de relatório de conhecimento (na página 1005)
Relatórios com base na web (na página 1006)
Formulários da Web de relatórios com base em função (na página 1006)

Ficha de relatório de conhecimento

A Ficha de relatório de conhecimento exibe informações sobre a contribuição de conhecimento de cada usuário final e oferece feedback sobre quais documentos de conhecimento foram mais efetivos. É possível usar a informação para melhorar os processos de criação de documentos de conhecimento e fornecer o melhor suporte para os usuários finais em seu ambiente.

Definir estatística de Ficha de relatório de documento de conhecimento

Use a página Ficha de relatório de documento de conhecimento para definir o cronograma de cálculo do produto e de envio de notificações sobre a Ficha de relatório de documento de conhecimento e para definir o conteúdo de emails de notificação da Ficha de relatório de documento de conhecimento.

Observação: as versões de trabalho e os documentos desativados não são apresentados quando o cálculo de Ficha de relatório de documento de conhecimento é executado.

Para definir estatísticas de Ficha de relatório de conhecimento

1. Na guia Administração, selecione Conhecimento, Ficha de relatório de documento de conhecimento.

   A página Ficha de relatório é aberta.

2. Preencha os campos a seguir conforme apropriado.

   Última atualização

   Executa cálculo do Relatório de atividades

   Padrão: Desativado

   Observação: se o cálculo não for executado e os dados estatísticos a serem apresentados não forem coletados, a seguinte mensagem aparecerá quando o comando Ficha de relatório de conhecimento for especificado no menu Exibir na guia Conhecimento: "Executar cálculo de ficha de relatório".

   Cronograma

   Programa a Ficha de relatório.

   - **O próximo Cálculo da ficha de Relatório será executado em xxx e a cada xxx** -- Especifica a frequência com que a estatística de Ficha de relatório será recalculada.

- **As notificações por email de Ficha de relatório serão enviadas em xxx e a cada xxx** -- Especifica a frequência com que as notificações de ficha de relatório serão enviadas.

  Padrão: Nunca

- **O email de Ficha de relatório deve exibir estatísticas dos últimos xxx —** especifica o período de tempo para o qual a notificação da Ficha de relatório contém informações. Esse campo só está disponível quando se seleciona um valor diferente da lista Nunca as notificações por email de Ficha de relatório serão enviadas a cada xxx.

  Padrão: 365 dias

3. Clique em Salvar.

   As estatísticas de Ficha de relatório de conhecimento são definidas.

Relatórios com base na web

O CA Business Intelligence instala um conjunto de relatórios Gerenciamento de conhecimento predefinidos. Esses relatórios são automaticamente implementados no servidor de criação de relatórios do BusinessObjects após a instalação do CA SDM.

Os relatórios são desenvolvidos com o BusinessObjects Web Intelligence ou o Crystal Reports. Os usuários autorizados podem exibir os relatórios nas guia Relatórios do CA SDM.

Formulários da Web de relatórios com base em função

É possível definir os formulários da web de relatório exibidos quando um gerente ou analista autorizado clica no ícone Lista de relatórios na guia Relatórios.

Os formulários da web de relatório são gerenciados através da Lista de funções no seguinte local: Administração, Gerenciamento de segurança e função, Gerenciamento de função.

Pesquisar

O recurso Pesquisa permite que os administradores executem as seguintes tarefas:

- Gerenciar o mecanismo de pesquisa Gerenciamento de conhecimento e definir as configurações usadas para gerenciar as palavras não pesquisáveis, termos especiais e sinônimos que foram incluídas ou excluídas das pesquisas.
- Definir as configurações usadas para analisar os documentos.
- Definir as configurações padrão da pesquisa.
- Criar "documentos recomendados" que são exibidos nos resultados da pesquisa. A listagem de FAQ dinâmica é usada para promover (intensificar) os documentos recomendados pra os usuários.

  Observação: um documento pode ter diferentes permissões que os anexos vinculados ao documento.

Consulte também

Mecanismo de pesquisa do KT (na página 1007)
Documentos recomendados (na página 1020)
Defina as opções de pesquisa padrão (na página 1025)

Mecanismo de pesquisa do KT

Após instalar o CA SDM, o mecanismo de pesquisa do KT é configurado como padrão. As pesquisas da base de conhecimento são limitadas aos documentos de conhecimento. O mecanismo de pesquisa está localizado na guia Administração, em Conhecimento, Pesquisa, nó do Mecanismo de pesquisa do KT.

O nó do Mecanismo de pesquisa do KT permite gerenciar as seguintes opções:

- Palavras não pesquisáveis
- Termos especiais
- Sinônimos

Mais informações:

Use a Pesquisa do Gerenciamento de conhecimento (na página 1008)

Use a Pesquisa do Gerenciamento de conhecimento

Após instalar o CA SDM, o mecanismo de pesquisa do Gerenciamento de conhecimento é configurado como o mecanismo de pesquisa padrão. As pesquisas da base de conhecimento são limitadas aos documentos de conhecimento.

É possível definir a acessibilidade e os padrões para todas as fontes de conhecimento com base em uma função de usuário. Por padrão, os documentos de conhecimento são pesquisáveis por todas as funções de usuário.

Siga estas etapas:

1. Clique na guia Administração.

   O Console de administração aparece.

2. Clique em Gerenciador de opções, Mecanismo de pesquisa.

   A página Lista de opções aparece.

3. Clique em ebr_version.

   A página Detalhes de opções aparece.

   Clique em Editar. A página Atualizar opções é exibida.

4. Selecione o mecanismo de pesquisa do KT.

5. Clique em Salvar, Atualizar.

   A página Detalhe de opções é atualizada com sua seleção.

6. Clique em Fechar janela.

7. Reinicie os serviços do CA SDM.

Consulte também

Palavras não pesquisáveis, sinônimos e termos especiais (na página 1009)
Criar palavras não pesquisáveis (na página 1010)
Editar uma palavra não pesquisável (na página 1010)
Exibir palavras não pesquisáveis (na página 1011)
Criar um termo especial (na página 1012)
Editar um termo especial (na página 1013)
Exibir termos especiais (na página 1013)
Criar um sinônimo (na página 1014)
Exibir sinônimos (na página 1015)
Editar um sinônimo (na página 1016)
Configurações de análise (na página 1016)

Palavras não pesquisáveis, sinônimos e termos especiais

É possível definir palavras (sinônimos, palavras não pesquisáveis e termos especiais) que afetam as pesquisas de palavra-chave e os idiomas naturais realizadas no CA SDM. A adição ou exclusão dos termos a seguir tem um efeito significativo nos resultados de pesquisa retornados para o usuário:

Palavras não pesquisáveis

Especifica palavras que geralmente não contribuem para o processo de pesquisa e podem, portanto, ser ignoradas. Por exemplo, termos como um, uma, o, a, ou e para frequentemente são identificadas como palavras não pesquisáveis. Use a página Lista de palavras não pesquisáveis para especificar palavras que o produto pode ignorar em documentos e consultas sem afetar o resultado da pesquisa.

Termos especiais

Especifica um termo que deve ser identificado como uma única palavra durante o processo de pesquisa, embora possa conter diversas palavras ou caracteres especiais. Por exemplo, palavras que têm um caractere que não seja alfanumérico, como barra normal (/) em TCP/IP, hífen (-) em dial-up ou sublinhado em LOCAL_SERVER. Em sua avaliação sobre quais palavras devem ser definidas como termos especiais, considere palavras válidas que podem ser divididas durante o processo de pesquisa uma vez que elas têm um caractere que não é alfanumérico.

Sinônimos

Especifica uma palavra que possui o mesmo significado de outra. É possível adicionar um sinônimo para quando um usuário pesquisar uma palavra específica e existir um sinônimo correspondente para ela em sua base de conhecimento, a informação pode ser encontrada. É possível definir vários sinônimos para a mesma palavra. O sistema cria automaticamente sinônimos reversos a partir das palavras-chave definidas. Por exemplo, caso defina computador como sinônimo da palavra PC, PC automaticamente se torna um sinônimo da palavra computador. Use a página Lista de sinônimos para especificar pares de sinônimos/palavras-chave que o produto usa de forma equivalente ao analisar documentos e consultas. Esses pares de sinônimos/palavras-chave podem melhorar os resultados de pesquisas.

Observação: após criar, modificar ou excluir palavras não pesquisáveis, termos especiais, sinônimos ou configurações de análise, use o utilitário de reindexação de documentos de conhecimento fornecido com o produto para reindexar a base de conhecimento.

Criar palavras não pesquisáveis

Use a página Criar nova palavra não pesquisável para adicionar uma nova palavra à lista de palavras que o produto pode ignorar em documentos e consultas sem afetar os resultados da pesquisa.

Para criar uma palavra não pesquisável

1. Na guia Administração, selecione Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Palavras não pesquisáveis.

   A página Lista palavras não pesquisáveis é exibida.

2. Clique em Criar novo.
3. A página Criar palavra não pesquisável é exibida.
4. Digite a palavra que deseja definir como uma palavra não pesquisável no CAMPO Palavra não pesquisável.

   Observação: você não pode definir uma palavra não pesquisável que exista como um sinônimo de uma palavra-chave.

5. Clique em Salvar

   A nova palavra não pesquisável atualizada é exibida na página Lista de palavras não pesquisáveis. É possível usar o botão Editar para atualizar a nova palavra não pesquisável.

Observação: após criar, modificar ou excluir palavras não pesquisáveis, termos especiais, sinônimos ou configurações de análise, use o utilitário de reindexação de documentos de conhecimento fornecido com o produto para reindexar a base de conhecimento.

Editar uma palavra não pesquisável

É possível editar uma palavra não pesquisável que já foi criada na página Lista de arquivos.

Observação: após criar, modificar ou excluir palavras não pesquisáveis, termos especiais, sinônimos ou configurações de análise, use o utilitário de reindexação de documentos de conhecimento fornecido com o produto para reindexar a base de conhecimento.

Para editar uma palavra não pesquisável

1. Clique com o botão direito do mouse na palavra não pesquisável desejada na lista Palavras não pesquisáveis e selecione Propriedades no menu de atalho.

   A página Atualizar palavras não pesquisáveis é aberta.

2. Digite suas mudanças no campo Palavra não pesquisável.

   Observação: você não pode definir uma palavra não pesquisável que exista como um sinônimo de uma palavra-chave.

3. Clique em Salvar.

   A palavra não pesquisável atualizada é exibida na página Lista de palavras não pesquisáveis.

Observação: após definir, modificar ou excluir palavras não pesquisáveis, termos especiais, sinônimos ou configurações de análise, use o utilitário de reindexação de documentos de conhecimento fornecido com o produto para reindexar a base de conhecimento.

Exibir palavras não pesquisáveis

Você pode exibir as informações de resumo para cada palavra não pesquisável na página Lista de palavras não pesquisáveis.

Para exibir as informações de resumo para cada palavra não pesquisável, selecione a guia Administração, então Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Palavras não pesquisáveis.

A página Lista de palavras não pesquisáveis é mostrada e exibe os seguintes campos:

Palavra não pesquisável

Define uma palavra não pesquisável pela qual procurar. Esse campo só é exibido quando você clica em Mostrar filtro.

Argumentos de pesquisa adicionais

Define os critérios adicionais pelos quais se deve pesquisar. Esse campo só é exibido quando você clica em um link Mais na página Pesquisa de conhecimento.

Lista de palavras não pesquisáveis

Exibe palavras para ignorar palavras em solicitações de pesquisa. A lista é exibida quando você clica no botão Pesquisar. Se digitar uma palavra no campo Palavra não pesquisável, a lista só exibirá a palavra especificada. Se você não digitou nada no campo Palavra não pesquisável, a lista exibirá todas as palavras não pesquisáveis definidas para o produto.

A partir da página Lista de palavras não pesquisáveis, é possível realizar as seguintes tarefas:

- Criar palavras não pesquisáveis (na página 1010)
- Editar uma palavra não pesquisável (na página 1010)

Criar um termo especial

Use a página Criar termo especial para especificar uma palavra ou frase que o produto deve tratar como palavras-chave únicas ao analisar documentos e consultas.

Para criar um termo especial

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Termos especiais.

   A página Lista de termos de especiais é exibida.

2. Clique em Criar novo.

   A página Criar termo especial é exibida.

3. Digite a palavra ou frase que deseja definir como um termo especial no campo Termo Especial.

4. Clique em Salvar.

   A página Criar termo especial é fechada e a página Detalhes do termo especial é aberta para que seja possível revisar a palavra ou frase adicionada. É possível usar o botão Editar para atualizar o novo termo. O novo termo especial é exibido na página Lista de termos especiais.

Editar um termo especial

É possível editar um termo especial.

Para editar um termo especial

1. Clique com o botão direito do mouse no termo que deseja editar na lista e selecione Editar no menu de atalho.

   A página Atualizar o termo especial é exibida.

2. Digite a palavra ou frase que deseja definir como um termo especial no campo Termo Especial.

3. Clique em Salvar.

   A página Atualizar termo especial é fechada e a página Detalhes do termo especial é aberta para que seja possível revisar a palavra ou frase adicionada. O termo atualizado é exibido na página Lista de termos especiais.

Exibir termos especiais

É possível exibir as informações do resumo para cada termo especial.

Para visualizar os termos especiais, selecione a guia Administração, então selecione Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Termos especiais.

A página Lista de termos especiais é exibida e é possível usar os seguintes campos para modificar os termos exibidos por padrão ou definir seus próprios:

Termo especial

Define um termo especial pelo qual procurar. Esse campo só é exibido quando você clica em Mostrar filtro.

Argumentos de pesquisa adicionais

Define os critérios adicionais pelos quais se deve pesquisar. Esse campo só é exibido quando você clica no link Mais no painel Pesquisa de conhecimento.

Termos especiais

Exibe palavras ou frases que contêm espaços ou caracteres (como hífens, barras e assim por diante) que o produto trata como palavras-chave únicas quando analisar consultas. Se tiver digitado uma palavra no campo Termo especial antes de clicar em Pesquisar, a lista só exibirá a palavra especificada. Se você não tiver digitado nada no campo Termo especial, a lista exibirá todos os termos especiais não pesquisáveis definidos para o produto.

A partir da página Lista de termos especiais, é possível realizar as seguintes tarefas:

- Criar um termo especial (na página 1012)
- Editar um termo especial (na página 1013)

Criar um sinônimo

Os sinônimos são palavras ou frases que têm o mesmo ou quase o mesmo significado da palavra-chave com a qual estão associados.

Se você definir um novo sinônimo complexo (isto é, um sinônimo contendo várias palavras separadas por espaços ou outros delimitadores), crie também um termo especial idêntico para que o produto possa tratar o sinônimo como uma única entidade. Por exemplo, se você definir "Computer Associates" como um sinônimo para "CA", defina também "Computer Associates" como um termo especial.

Observação: você não pode definir um sinônimo ou palavra-chave que exista como uma palavra não pesquisável.

Para criar um sinônimo

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Sinônimos.

   A página Lista de sinônimos é exibida.

2. Clique em Criar novo.

   A página Criar sinônimo é exibida.

3. Digite a palavra ou frase que deseja definir como sinônimo no campo Sinônimo.

4. Clique em Salvar.

   A página Criar sinônimo é fechada e a página Detalhes do sinônimo é aberta para que seja possível revisar a palavra ou frase adicionada. O novo sinônimo é exibido na página Lista de sinônimos.

Exibir sinônimos

É possível exibir as informações do resumo para cada sinônimo.

Para visualizar os sinônimos, selecione a guia Administração, então selecione Conhecimento, Pesquisa, Mecanismo de pesquisa do KT, Sinônimos.

A página de Lista de sinônimos é exibida e é possível modificar as palavras-chave exibidas por padrão, ou definir suas próprias usando os seguintes campos:

Palavra-chave

Define uma palavra-chave pela qual procurar. Esse campo só é exibido quando você clica em Mostrar filtro.

Sinônimo

Define um sinônimo pelo qual procurar. Esse campo só é exibido quando você clica em Mostrar filtro.

Argumentos de pesquisa adicionais

Define os critérios adicionais pelos quais se deve pesquisar. Esse campo só é exibido quando você clica no link Mais no painel Pesquisa de conhecimento.

Lista de sinônimos

Exibe pares de sinônimos/palavras-chave definidos no produto. Para cada palavra-chave exibida na coluna Palavra-chave, a coluna Sinônimo exibirá um ou mais sinônimos.

A partir da página Lista de sinônimos, é possível realizar as seguintes tarefas:

- Criar um sinônimo (na página 1014)
- Editar um sinônimo (na página 1016)

Editar um sinônimo

É possível editar um sinônimo.

Para editar um sinônimo

1. Clique com o botão direito do mouse no termo desejado na lista e selecione Editar no menu de atalho.

   A página Atualizar sinônimo é exibida.

2. Digite a palavra ou frase que deseja definir como um termo especial no campo Sinônimo.
3. Clique em Salvar.

   A página Atualizar sinônimo é fechada e a página Detalhes do sinônimo é aberta para que seja possível revisar a palavra ou frase adicionada. O termo atualizado é exibido na página Lista de sinônimos.

Configurações de análise

Ao publicar um documento na base de conhecimento, o produto analisa as informações nos campos Título, Resumo, Problema e Resolução do documento para torná-las palavras-chave. Quando um usuário pesquisa a base de conhecimento, o produto compara as palavras-chave da consulta do usuário às palavras-chave analisadas da base de conhecimento para produzir uma lista de resultados. A página Configurações de análise permite definir as configurações usadas para analisar documentos na base de conhecimento.

Observação: o recurso de Configurações de análise está disponível apenas com o mecanismo de pesquisa do KT padrão.

Definir configurações de análise

Ao publicar um documento na base de conhecimento, o produto analisa as informações nos campos Título, Resumo, Problema e Resolução do documento para torná-las palavras-chave. Quando um usuário pesquisa a base de conhecimento, o produto compara as palavras-chave da consulta do usuário às palavras-chave analisadas da base de conhecimento para produzir uma lista de resultados.

Para definir as configurações usadas para analisar os documentos na base de conhecimento, navegue até a guia Administração em Conhecimento, Pesquisa, Configurações de análise.

As Configurações de análise são exibidas e é possível usar os seguintes campos para definir as configurações:

Máximo de palavras-chave para pesquisa

Define o número máximo de palavras-chave a extrair quando o produto analisa o texto de pesquisa.

Padrão: 20

Observação: o intervalo válido é de 1 a 100, de modo que o administrador de conhecimento do CA SDM pode alterar o valor dentro desse intervalo com base em necessidades de pesquisa e parâmetros de um banco de dados de conhecimento específico. Use um número mais baixo de palavras-chave de pesquisa para obter um desempenho mais rápido.

Idioma

Especifica o tipo de idioma a usar para o processamento da análise. Selecione uma das seguintes configurações:

Inglês

Executa certos tipos de processamento específicos da língua inglesa (por exemplo, ignorar o plural de termos de pesquisa) durante uma pesquisa, se aplicável.

Outros europeus

Executa somente o processamento específico de idiomas europeus durante a pesquisa.

Coreano

Executa somente o processamento específico de coreano durante a pesquisa.

Outro Extremo Oriente

Realiza o processamento para os outros idiomas do oriente durante a pesquisa.

Observação: quando estiver em um ambiente operacional chinês, japonês ou coreano, verifique se você compreende as abordagens de análise disponíveis e as limitações dos idiomas MBCS (na página 1020), antes de implementar seu sistema Gerenciamento de conhecimento para ajudar a garantir as expectativas do usuário sejam estabelecidas de maneira adequada.

Intervalo válido de caracteres

Define o intervalo de caracteres alfanuméricos a considerar válido na análise de campos Título, Resumo, Problema e Resolução em um documento. O produto trata quaisquer outros caracteres como separadores.

Observação: quando você seleciona Sim na lista Reconhecer termos especiais, o produto não analisa palavras e frases definidas como termos especiais.

Padrão: a-z, que indica que os caracteres alfabéticos a até z são caracteres válidos para análise.

O campo Intervalo válido de caracteres contém as letras adequadas que a análise usa. As letras não apresentadas no Intervalo válido de caracteres serão removidas.

Os valores recomendados para idiomas são:

Idioma	Intervalo válido de caracteres
Alemão	a-zäöüß
Espanhol	a-záéíóúüñ
Francês	a-zàäâçéèêëĩïôùû
Português do Brasil	a-zàáãçéêíóúü
Italiano	a-zàèéìĩïù
Chinês simplificado	a-z
Japonês	a-z
Chinês tradicional	a-z
Coreano	a-z

Observação: o japonês contém o intervalo de “a-z” mais uma lista de caracteres Katakana válidos, excluindo os sinais de pontuação.

Remover palavras similares

Especifica se o produto remove palavras-chave estruturalmente semelhantes dos grupos usados em uma pesquisa. É possível selecionar uma das seguintes configurações:

Sim

Remove palavras-chave estruturalmente semelhantes dos critérios de pesquisa.

Observação: quando você seleciona Sim, o produto também remove palavras similares ao salvar ou publicar o documento. Essa configuração pode afetar se um documento é pesquisável caso o campo Remover palavras similares esteja definido como Sim. A palavra similar pode não ter sido indexada e usada na pesquisa e recuperação posteriores do documento.

Não

Mantém palavras-chave estruturalmente semelhantes nos critérios de pesquisa.

Padrão: Não

Remover palavras não pesquisáveis

Especifica se o produto remove palavras não pesquisáveis quando analisar os campos Título, Resumo, Problema e Resolução em um documento. É possível selecionar uma das seguintes configurações:

Sim

Remove palavras não pesquisáveis dos critérios de pesquisa.

Não

Mantém palavras não pesquisáveis nos critérios de pesquisa.

Padrão: Sim

Reconhecer termos especiais

Especifica se o produto considera termos especiais como entidades únicas ou como várias palavras quando analisar os campos Título, Resumo, Problema e Resolução em um documento. É possível selecionar uma das seguintes configurações:

Sim

Processa termos especiais como entidades únicas nos critérios de pesquisa.

Não

Processa as palavras que abrangem termos especiais como entidades separadas nos critérios de pesquisa.

Padrão: Sim

Limitações de pesquisa do conjunto de caracteres de bytes múltiplos

Certifique-se de compreender as abordagens de análise disponíveis e as limitações das linguagens MBCS antes de implementar o sistema Gerenciamento de conhecimento para ajudar a garantir que as expectativas do usuário sejam definidas de maneira adequada. Essa limitação do produto tem impacto nos recursos de pesquisa usando os textos nos idiomas japonês, chinês ou coreano no sistema. O mecanismo de análise de palavra usado pelo mecanismo de pesquisa é controlado na página Configurações de análise (na página 1016).

Para as configurações de inglês, coreano e outros idiomas europeus, o produto assume a pontuação, “espaço em branco" ou ambos os caracteres separam as palavras. Essa suposição permite que o texto do documento seja desdobrado em palavras específicas e permite que palavras não pesquisáveis sejam ignoradas, ocorrendo a aplicação de sinônimos conhecidos e termos especiais para os termos de pesquisa.

Como alternativa, quando a configuração para idioma do Extremo Oriente é selecionada, a rotina de análise usa uma abordagem caractere por caractere para se adaptar a algumas abordagens de texto de idiomas do Extremo Oriente, não usando delimitadores de espaço em branco entre as palavras. Essa configuração diz ao analisador para assumir que cada caractere é tratado como uma palavra completa. A configuração é aplicada a todo o texto a ser pesquisado. Em virtude de as configurações alterarem a maneira como a análise de pesquisa funciona, todo o índice de pesquisa precisa ser recriado caso as configurações de idioma sejam alteradas de ou para um idioma do Extremo Oriente.

Documentos recomendados

Os usuários do CA SDM podem especificar um critério sobre um item de interesse e o mecanismo de pesquisa encontra documentos de conhecimento correspondentes e os exibe na página de resultado de pesquisa como um conjunto de links de "documentos recomendados". A consulta da pesquisa pode ser expressa como uma palavra-chave ou um conjunto de palavras (frase) que identifica o conceito desejado que um ou mais documentos podem conter.

A lista de documentos que atende aos critérios de pesquisa é organizada e classificada (do maior para o menor) para colocar os documentos mais relevantes no início dos resultados da pesquisa. Usar os documentos recomendados ajuda os usuários a reduzirem o tempo necessário para encontrar as informações desejadas.

Para fornecer um conjunto de documentos correspondentes que são classificados de acordo dom com alguns critérios rapidamente, o mecanismo de pesquisa coleta dados pelo tipo de condição (frase, palavras-chave ou categoria) que o administrador configura na página Criar documentos recomendados.

Mais informações:

Criar documentos recomendados (na página 1021)
Editar uma condição de um documento recomendado (na página 1023)
Exibir documentos recomendados (na página 1023)
Pesquisar documentos recomendados (na página 1024)

Criar documentos recomendados

Os administradores podem criar documentos recomendados que os usuários podem encontrar ao especificar os critérios sobre um item de interesse.

Observação: se multilocação estiver instalada, selecione o inquilino apropriado na lista suspensa. A opção Público (compartilhado) cria o objeto para todos os inquilinos.

Para criar um documento recomendado

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Documentos recomendados.

   A Lista de documentos recomendados aparece.

2. Clique em Criar novo.

   A página Criar documentos recomendados é exibida.

3. Preencha os campos a seguir conforme apropriado.

   Documento de conhecimento

   Especifica um documento de conhecimento ou clique no ícone de pesquisa para abrir a página Pesquisa de documento de conhecimento.

Tipo de condição

Especifica um tipo de condição (na página 1022) pelo qual o mecanismo de pesquisa classifica e indica a correspondência do documento.

- Se o tipo de condição for Correspondência exata, Frase exata ou Palavras-chave, um campo de texto é exibido. É possível inserir uma frase ou palavra-chave que identifique o conceito que deseja que o documento contenha.
- Se o tipo de condição for Categoria do documento de conhecimento, o link Categoria do documento de conhecimento é exibido. É possível especificar uma categoria de conhecimento para ser associada a esse documento.

Status

Define o status desse registro como ativo ou inativo.

Clique em Salvar.

O novo arquivo recomendado é salvo na base de conhecimento e é exibido na página Lista de documentos recomendados.

Campo tipo de condição

O mecanismo de pesquisa localiza os documentos de acordo com os seguintes tipos de condição:

Correspondência exata

Pesquisa por documentos de acordo com a frase inserida no texto de pesquisa. Uma correspondência ocorre apenas quando o mecanismo de pesquisa localiza todas as palavras especificadas em uma frase.

Frase exata

Pesquisa por documentos de acordo com a frase exata inserida no texto de pesquisa. Uma correspondência ocorre apenas quando o mecanismo de pesquisa localiza o conjunto exato ou sequência de palavras em uma frase.

Palavras-chave

Pesquisa por documentos de acordo com as palavras-chave no texto de pesquisa. Uma correspondência ocorre apenas quando o mecanismo de pesquisa localiza todas as palavras-chave.

Knowledge Category

Pesquisa por documentos de acordo com a categoria de conhecimento. Uma correspondência ocorre apenas quando o usuário navega para uma categoria configurada para os documentos recomendados.

Editar uma condição de um documento recomendado

É possível atualizar uma condição de documento recomendado.

Para editar a condição de um documento recomendado

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Documentos recomendados.

   A página Lista de documentos recomendados é exibida.

2. Para editar uma condição, clique com o botão direito do mouse no título na coluna Condição.

   A página Atualizar documento recomendado é exibida.

3. Preencha os campos conforme apropriado.
4. Clique em Salvar.

   A condição atualizada é exibida na lista Documentos recomendados.

Exibir documentos recomendados

É possível exibir as informações do resumo para cada documento recomendado.

Para exibir os documentos recomendados, selecione Pesquisa, e Documentos recomendados na guia Administração.

A página Lista de documentos recomendados é exibida e inclui as seguintes colunas:

Condição

Indica o tipo de condição pelo qual o mecanismo de pesquisa classifica e indica a correspondência do documento.

Documento de conhecimento

Exibe os documentos no conjunto de resultados.

Autor

Define um autor do documento de conhecimento.

Data de modificação

Exibe a data em que o documento foi modificado pela última vez.

A partir da página Lista de documentos recomendados, é possível realizar as seguintes tarefas:

- Criar um documento recomendado (na página 1021)
- Editar uma condição de um documento recomendado (na página 1023)
- Pesquisar documentos recomendados (na página 1024)

Pesquisar documentos recomendados

É possível usar a função de pesquisa para filtrar a Lista de documentos recomendados para mostrar apenas os itens que deseja consultar.

Observação: se multilocação estiver instalada, a página de lista exibirá configurações de dados públicos e de inquilino no filtro de pesquisa. Dados públicos podem ser Excluídos ou Incluídos com dados de inquilino; Pesquisa apenas objetos públicos exclusivamente. Nas páginas de detalhes, selecione o inquilino apropriado na lista. Se selecionar <vazio>, o objeto é público.

Para pesquisar um documento recomendado

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Resultados recomendados.

   A Lista de documentos recomendados aparece.

2. Clique em Mostrar filtro.
3. Preencha os campos conforme apropriado. Os seguintes campos exigem mais explicação.

   Tipo

   Especifica um tipo de condição pelo qual o documento é correspondido e exibido como um link de documento recomendado.

   Phrase/Keywords

   Especifica a informação para consulta da pesquisa pela qual é identificado o conceito desejado contido no documento.

   Clique em Pesquisar.

   A Lista de documentos recomendados é preenchida com todos os itens que correspondem aos critérios de pesquisa.

Defina as opções de pesquisa padrão

É possível definir as opções de pesquisa a serem usadas como opções padrão que são exibidas quando os usuários pesquisam pelo conhecimento usando o campo de pesquisa.

Observação: essas opções de pesquisa são sobrescritas por quaisquer configurações definidas pelo usuário na janela Preferências, ou quaisquer opções de pesquisa adicionais na seção de Pesquisa de conhecimento ou no painel de Categorias na guia Administração.

Para definir as opções de pesquisa padrão

1. Na guia Administração, navegue até Conhecimento, Pesquisa, Configurações de pesquisa.

   A página Opções de pesquisa é exibida.

2. Selecione as seguintes opções conforme apropriado:

   Resultados recomendados

   Especifica o número de documentos a serem exibidos na lista de resultados de pesquisa.

   Campos de pesquisa padrão

   Especifica quais campos do documento incluir por padrão em pesquisas por palavra-chave. Marque uma caixa de seleção para incluir o campo associado em pesquisas padrão. Desmarque uma caixa de seleção para excluir o campo associado de pesquisas padrão. Os seguintes campos de documento estão disponíveis para a pesquisa:

   - Título
   - Resumo
   - Problema
   - Resolução
   - Anexos

   Configurações de pesquisa para todas as origens

   Especifica se as pesquisas podem incluir todas as origens do documento de conhecimento. Por exemplo, categorias de conhecimento e áreas de solicitação.

Configurações de pesquisa no contexto de um ticket

Especifica se as pesquisas podem incluir todos os campos definidos em um ticket da central de serviços (incidente, problema, ocorrência, requisição de mudança ou solicitação).

- Para essas opções, selecione *um* dos seguintes tipos de correspondência:
  - **Qualquer uma das palavras (OR) —** inclui um documento no conjunto de resultados quando ele contém qualquer uma das palavras no campo Pesquisa. Essa opção é a seleção padrão.
  - **Todas as palavras (AND) —** inclui um documento no conjunto de resultados apenas quando ele contém todas as palavras no campo Pesquisa.

Clique em Salvar.

As configurações padrão de pesquisa são definidas.

Opções de integração do CA SDM

As seguintes opções de configuração estão disponíveis para a integração do CA SDM:

Mapeamento de campos

Especifica quais campos do CA SDM devem ser preenchidos com informações do Gerenciamento de conhecimento e se as informações existentes devem ser sobrescritas.

Configuração de pesquisa de ocorrências

Seleciona os campos a pesquisar ao clicar no botão Pesquisar conhecimento em um ticket.

Configuração de pesquisa de ocorrências de solicitação

Seleciona os campos a pesquisar ao clicar no botão Pesquisar em um ticket.

Configuração de pesquisa de solicitação/incidente/problema

Seleciona os campos a pesquisar ao clicar no botão Pesquisar em um ticket.

Sugerir conhecimento

Seleciona os campos a pesquisar ao clicar em Exibir conhecimento antes do botão Salvar em um ticket.

Mais informações:

Definir mapeamento de campo (na página 1027)
Definir configuração de pesquisa de ocorrências (na página 1030)
Definir configuração de pesquisa de solicitação/incidente/problema (na página 1031)
Sugestões de conhecimento (na página 1032)
Definir categorias de ocorrência (na página 1033)
Definir as áreas de solicitação/incidente/problema (na página 1034)
Configurar políticas de Autoatendimento (na página 1035)

Definir mapeamento de campo

Os administradores podem usar a seção Mapeamento de campos para especificar quais campos devem ser preenchidos com informações do Gerenciamento de conhecimento, e se as informações existentes devem ser substituídas.

Para definir campos no service desk para o Gerenciamento de conhecimento

1. Na guia Administração, navegue até Conhecimento, Integração com o Service Desk, Mapeamento de campos.

   A página Mapeamento de campo aparece.

2. Preencha os campos a seguir conforme apropriado:

   Preencher valores do Service Desk a partir do Gerenciamento de conhecimento

   Especifica se as informações do Gerenciamento de conhecimento devem ser usadas para preencher campos em ocorrências ou solicitações do service desk.

   - Marque a caixa de seleção para disponibilizar os campos do Gerenciamento de conhecimento colunas Preencher valores vazios do Service Desk e Sobrescrever valores do Service Desk. Com isso, você pode especificar quais informações do Gerenciamento de conhecimento devem ser usadas para preencher campos em ocorrências ou solicitações do service desk.
   - Desmarque a caixa de seleção para tornar os campos Preencher valores vazios do Service Desk e Sobrescrever valores do Service Desk do Gerenciamento de conhecimento indisponíveis. Neste caso, os usuários devem preencher manualmente as ocorrências do service desk ou as solicitações criadas no Gerenciamento de conhecimento.

   Padrão: esta caixa de seleção é marcada.

   Service Desk

   Identifica os campos em ocorrências ou solicitações que correspondem a campos listados na coluna do Gerenciamento de conhecimento.

   Para cada caixa de seleção marcada na coluna Preencher valores vazios do Service Desk, as informações do campo correspondente na coluna Gerenciamento de conhecimento preencherão a ocorrência ou solicitação.

   Gerenciamento de conhecimento

   Identifica os campos do Gerenciamento de conhecimento que correspondem aos campos da central de serviços listados na coluna Service Desk.

   Para cada caixa de seleção marcada na coluna Preencher valores vazios do Service Desk, as informações do campo correspondente na coluna Gerenciamento de conhecimento preencherão a ocorrência ou solicitação.

A coluna Gerenciamento de conhecimento contém duas listas suspensas:

- A primeira lista suspensa corresponde ao campo Resumo na coluna Service Desk e especifica o campo do Gerenciamento de conhecimento (Título, Resumo ou Problema) que deve ser usado para preencher o campo Resumo em uma ocorrência ou solicitação.

Padrão: resumo.

- A segunda lista suspensa corresponde ao campo Descrição na coluna Service Desk e especifica o campo do Gerenciamento de conhecimento (Título, Resumo ou Problema) que deve ser usado para preencher o campo Descrição em uma ocorrência ou solicitação.
- **Padrão:** problema.

Preencher valores vazios do Service Desk

Especifica quais campos vazios em uma ocorrência ou solicitação da central de serviços devem ser preenchidos com informações do Gerenciamento de conhecimento.

- Marque uma caixa de seleção para mapear informações do campo do Gerenciamento de conhecimento para o campo Service Desk correspondente se este não contiver informações atualmente.
- Desmarque uma caixa de seleção se não deseja mapear informações do campo do Gerenciamento de conhecimento para o campo correspondente da central de serviços.

Padrão: As caixas de seleção correspondentes aos campos

Resumo, Descrição, Produto, Ativo e Área de solicitação na central de serviços são selecionados.

Sobrescrever valores do Service Desk

Especifica quais campos em uma ocorrência ou solicitação da central de serviços devem ser sobrescritos com informações do Gerenciamento de conhecimento.

- Marque uma caixa de seleção para substituir as informações no campo Service Desk com informações do campo do Gerenciamento de conhecimento correspondente.
- Desmarque uma caixa de seleção caso não deseje substituir informações no campo Service Desk com as informações do campo do Gerenciamento de conhecimento correspondente.

Essas caixas de seleção ficam disponíveis apenas quando as caixas de seleção correspondentes na coluna Preencher valores vazios do Service Desk estão selecionadas.

Padrão: todas as caixas de seleção de substituição de valores do Service Desk são desmarcadas.

Clique em Salvar.

O mapeamento de campo é definido.

Definir configuração de pesquisa de ocorrências

É possível definir os campos em uma Ocorrência para pesquisar ao clicar no botão Pesquisar conhecimento em um ticket. Os campos selecionados são copiados para os campos correspondentes no Filtro de pesquisa na guia Conhecimento da janela Detalhes da ocorrência. O preenchimento dos campos Filtro de pesquisa do ticket ocorre quando a guia Conhecimento está selecionada ou ao clicar no botão Redefinir filtro (na guia Conhecimento).

Para definir os campos em uma Ocorrência a serem usados para pesquisas da base de conhecimento

1. Na guia Administração, selecione Conhecimento, Integração do CA SDM, Configuração de pesquisa de ocorrência.

   A página de Integração do CA SDM é exibida.

2. Selecione os campos que deseja que estejam disponíveis para pesquisas da Base de conhecimento.
   - Resumo
   - Descrição
   - Item de configuração
   - Prioridade
   - Categoria
   - Motivo raiz
   - Produto

   Observação: não é possível selecionar ambos os campos Resumo e Descrição.
3. Selecione a opção Executar automaticamente uma pesquisa quando a guia Conhecimento de uma ocorrência for selecionada caso deseje pesquisar a base de conhecimento automaticamente quando a guia Conhecimento na página de detalhes for selecionada.
4. Clique em Salvar.

   A pesquisa de ocorrência é configurada.

Definir configuração de pesquisa de solicitação/incidente/problema

É possível definir os campos em uma solicitação, incidente ou problema para pesquisar ao clicar no botão Pesquisa de conhecimento em um ticket. Os campos selecionados são copiados para os campos correspondentes no Filtro de pesquisa na guia Conhecimento da página de detalhes do ticket. O preenchimento dos campos Filtro de pesquisa do ticket ocorre quando a guia Conhecimento está selecionada ou ao clicar no botão Redefinir filtro (na guia Conhecimento).

Para definir os campos em uma solicitação, incidente ou problema a serem usados para pesquisas da base de conhecimento

1. Na guia Administração, selecione Conhecimento, Integração do CA SDM, Configuração de pesquisa de Solicitação/incidente/problema.

   A página de Integração do CA SDM é exibida.

2. Selecione os campos que deseja que estejam disponíveis para pesquisas da Base de conhecimento.

   - Resumo
   - Descrição
   - Item de configuração
   - Gravidade
   - Impacto
   - Urgência
   - Prioridade
   - Área de solicitação
   - Motivo raiz

   Observação: não é possível selecionar ambos os campos Resumo e Descrição.

3. Selecione a opção Executar automaticamente uma pesquisa quando a guia Conhecimento de uma solicitação for selecionada caso deseje pesquisar a base de conhecimento automaticamente quando a guia Conhecimento na página de detalhes for selecionada.

4. Clique em Salvar.

   São configurados os campos em uma solicitação, incidente ou problema a serem usados para buscar as pesquisas da base de conhecimento.

Sugestões de conhecimento

Os usuários e clientes podem, onde permitido, exibir uma lista das sugestões de conhecimento ao criarem um ticket na interface de autoatendimento.

Caso uma solução seja encontrada e o ticket não esteja salvo, os documentos que foram sugeridos podem ser creditados por um sistema de classificação de autoatendimento no formulário do documento. Esse sistema de classificação pode ser diferente dependendo das configurações de política de autoatendimento definida na página de Configuração de pesquisa.

Os dados recuperados podem ser usados para relatórios, painéis e também ao pesquisar a base de conhecimento em que os usuários podem filtrar os documentos que resolveram com sucesso seus tickets.

Os benefícios do autoatendimento estão na forma de menos chamadas de suporte e tickets redundantes criados, o que se traduz em custos operacionais reduzidos.

O administrador deve ativar esse recurso antes de usar e configurar a ocorrência adequada e solicitar áreas para as quais o conhecimento é sugerido na interface do autoatendimento.

Definir categorias de ocorrência

É possível definir as categorias de ocorrência para as quais o conhecimento é sugerido aos funcionários e clientes durante a criação do ticket.

É possível também marcar o recurso Sugerir conhecimento como ativo ou inativo. Quando você marca este recurso como inativo, ele se torna indisponível para os clientes e funcionários, mas permanece disponível no banco de dados para uso futuro. Se você decidir usar este recurso no futuro, você pode voltar e marcá-lo como ativo.

para definir a sugestão categorias de ocorrências de conhecimento

1. Na guia Administração, navegue até Conhecimento, Integração com o Service Desk, Conhecimento sugerido, Categorias de ocorrência.

   A página Sugerir conhecimento para categorias de ocorrências salvas é exibida.

2. Selecione a opção **Não sugerir conhecimento** para marcar o recurso Sugerir conhecimento como ativo.

   Padrão: Inativo

Caso marque esse recurso como ativo, as seguintes opções são exibidas:

Por padrão, o conhecimento será:

Sugerido

Indica se você *realmente* deseja que seja sugerido conhecimento para todas as categorias de ocorrência exceto as definições na lista de categorias de ocorrência.

Não sugerido

Indica se você *não* deseja que seja sugerido conhecimento para todas as categorias de ocorrência exceto as definições na lista de categorias de ocorrência.

Para todas as Categorias de ocorrência, exceto o seguinte:

Mostra a lista das áreas de solicitação em que o conhecimento é sugerido ou não sugerido a funcionários e clientes na interface de autoatendimento. O usuário de autoatendimento não é autorizado a editar as áreas de solicitação, elas são somente leitura.

3. Clique em *um* dos seguintes botões:

Adicionar

Adiciona a área de solicitação selecionada à lista.

Remover

Remove a área de solicitação selecionada da lista.

Remover tudo

Remove todas as áreas de solicitação da lista.

Salvar

Salva as informações da área de solicitação na base de conhecimento.

As categorias de ocorrência são definidas.

Definir as áreas de solicitação/incidente/problema

É possível definir as áreas de solicitação, problema e incidente para as quais o conhecimento é sugerido aos funcionários e clientes durante a criação do ticket.

É possível também marcar o recurso Sugerir conhecimento como ativo ou inativo. Quando você marca este recurso como inativo, ele se torna indisponível para os clientes e funcionários, mas permanece disponível no banco de dados para uso futuro. Se você decidir usar este recurso no futuro, você pode voltar e marcá-lo como ativo.

Para definir o conhecimento sugerido para áreas de solicitações/incidentes/problemas

1. Na guia Administração, navegue até Conhecimento, Integração com o CA SDM, Conhecimento sugerido, Áreas de solicitação/incidente/problema.

   A página Sugerir conhecimento para as áreas de solicitação/incidente/problema é exibida.

2. Selecione a opção **Não sugerir conhecimento** para marcar o recurso Sugerir conhecimento como ativo.

   Padrão: Inativo

   Caso marque esse recurso como ativo, algumas opções adicionais são exibidas:

   Por padrão, o conhecimento será:

   Sugerido

   > Especifique essa opção caso deseje que seja sugerido conhecimento para todas as áreas de solicitação/incidente/problema exceto para aquelas definidas na lista da Área de solicitação.

   Não sugerido

   > Especifique essa opção caso *não* deseje que seja sugerido conhecimento para todas as áreas de solicitação/incidente/problema exceto para aquelas definidas na lista da Área de solicitação.

   Para todas as áreas de solicitações/incidentes/problemas, exceto o seguinte:

   > Mostra a lista das áreas de solicitação em que o conhecimento é sugerido ou não sugerido a funcionários e clientes na interface de autoatendimento. O usuário de autoatendimento não é autorizado a editar as áreas de solicitação, elas são somente leitura.

Clique em Salvar.

A sugestão de conhecimento para as áreas de solicitação/incidente/problema é definida.

Configurar políticas de Autoatendimento

É possível configurar as políticas de autoatendimento que creditem documentos com base em um conjunto de cenários de usuário.

Configurar políticas de autoatendimento

1. Na guia Administração, navegue até Conhecimento, Integração com o CA SDM, Conhecimento sugerido, Configuração de autoatendimento.

   A página Configurações de pesquisa é exibida.

2. Especifica as configurações de política adequadas que credita documentos e salva os tickets rejeitados com base nos seguintes cenários de usuário:

   - O usuário não abriu nenhum documento sugerido
   - O usuário abriu um documento sugerido
   - O usuário aceitou um documento sugerido como solução para o problema
   - O usuário procurou conhecimento, abriu um documento e saiu

   Clique em Salvar.

   As configurações da política de autoatendimento são salvas.

Pesquisa de soluções

As Pesquisas de solução permitem que você colete e analise o feedback do cliente sobre o desempenho do Documento de conhecimento. É possível modificar as configurações de pesquisa ao selecionar Conhecimento, Pesquisa de solução na Interface administrativa. A pesquisa aparece em um Documento de conhecimento publicado e permite que os clientes, convidados e funcionários determinem a classificação de efetividade do Documento de conhecimento.

Esse recurso contém os seguintes componentes:

- Configurações do FAQ
- Configurações de pesquisa

Mais informações:

Definir configurações de perguntas frequentes (na página 1037)
Definir configurações da pesquisa de soluções (na página 1039)

Definir configurações de perguntas frequentes

Use a página Configurações de perguntas frequentes para definir os parâmetros usados pelo produto para calcular a classificação da pergunta frequente atribuída a cada documento. O produto baseia a classificação de perguntas frequentes nos seguintes critérios:

- Com que frequência o documento foi acessado no passado
- O quanto o documento foi útil para os usuários
- Como a eficácia do documento diminuiu ao longo do tempo

Por padrão, a página de lista de documentos exibe os documentos em ordem de classificação de perguntas frequentes (isso é, em ordem de utilidade). Os documentos mais úteis são exibidos no início da lista de documentos. Ao longo do tempo, os documentos tendem a descer na lista de documentos, à medida que os usuários aprendem soluções para os problemas.

Para definir as configurações de FAQ

1. Selecione Conhecimento, Pesquisa de soluções, Configurações de FAQ na guia administração.

   A página Configurações de FAQ é exibida.

2. Preencha os campos a seguir conforme apropriado:

   Última atualização

   Especifica se o serviço de Classificação das perguntas frequentes deve ser executado e exibe a data na qual as classificações de perguntas frequentes foram atualizadas pela última vez.

   - Marque a caixa de seleção Executar o serviço de Classificação das perguntas frequentes para executar o cálculo de perguntas frequentes usando as configurações nessa janela.
   - Desmarque a caixa de seleção Executar o serviço de Classificação das perguntas frequentes para desativar o cálculo de perguntas frequentes.

Cronograma

Define a frequência com que o produto atualiza as classificações das perguntas frequentes. Esse campo contém os seguintes componentes:

Executar o cálculo de perguntas frequentes a cada...

Especifica o tempo decorrido antes que o produto atualize a classificação das perguntas frequentes para documentos.

Padrão: 1 dia

De...

Especifica a hora do dia em que o produto deve começar a recalcular as classificações das perguntas frequentes.

Padrão: 00:00 (12:00 AM)

Para...

Especifica a hora do dia em que o produto deve parar de recalcular as classificações das perguntas frequentes, mesmo que o cálculo não esteja concluído.

Padrão: 07:00 (7:00 A.M.)

Observação: esta configuração começa a ter efeito no dia posterior à instalação do produto. Por exemplo, se você instalar o produto em 19 de abril de 2008, o servidor de perguntas frequentes é executado pela primeira vez em 20 de abril de 2008.

Vencimento

Define o número de vezes que a classificação de um FAQ de documento será recalculada antes que atinja 0. Com base no valor especificado, a classificação do FAQ do documento diminui e, eventualmente, torna-se 0, e neste ponto aparecerá na parte inferior da lista de documentos (quando a lista estiver classificada por Classificação de perguntas frequentes).

Padrão: 180

Por exemplo, se o valor Vencimento for 180 para um documento com a classificação 4 (muito útil), a classificação das perguntas frequentes do documento é 0 (zero) quando o produto tiver recalculado a classificação das perguntas frequentes 180 vezes.

Observação: por padrão, o cálculo de estatística das perguntas frequentes requer dados de bu_trans para os últimos 180 dias, onde 180 é o fator de envelhecimento. Portanto, se você alterar o fator de vencimento das perguntas frequentes para mais de 365 dias, deverá estender também as regras de arquivamento para a tabela de bu_trans.

Dias como novo

Especifica quantos dias um documento recém-criado ou importado é exibido na pasta Novos documentos na guia Conhecimento.

Padrão: 5 dias

Classificação

Especifica a classificação padrão (Nem um pouco útil, Um pouco útil ou Muito útil) para documentos que os usuários abriram mas não classificaram.

Padrão: Relativamente útil

Clique em Salvar.

As configurações de FAQ são definidas.

Definir configurações da pesquisa de soluções

Use a página de Configurações de pesquisa para configurar como um documento de conhecimento é exibido quando acessado para resolver um problema ou responder a uma pergunta.

Para definir configurações da pesquisa de soluções

1. Selecione Conhecimento, Pesquisa de soluções, Configurações de pesquisa na guia administração.

   A página Configurações da pesquisa é exibida.

2. Preencha os campos a seguir conforme apropriado. Clique em Salvar.

   As configurações de pesquisa de soluções são definidas.

Configurações do sistema Gerenciamento de conhecimento

É possível definir informações padrão para serem exibidas na guia Conhecimento (no logon), o formato que as categorias são exibidas na seção Categorias de conhecimento na guia Administração e o número de documentos na lista Principais soluções na página inicial do Gerenciamento de conhecimento.

Mais informações:

Definir configurações gerais (na página 1040)

Definir configurações gerais

É possível definir informações padrão para serem exibidas na guia Conhecimento no logon, o formato em que as categorias são exibidas na seção Categorias de conhecimento na guia Administração e o número de documentos na lista Principais soluções na página inicial do Gerenciamento de conhecimento.

Para definir as configurações gerais

1. Selecione Administração, Conhecimento, Sistema, Configurações gerais na seção esquerda da guia Administração.

   A página Configurações gerais é exibida.

2. Preencha as seguintes configurações conforme apropriado:

   Tela de abertura da ferramenta de pesquisa

   Especifica a informação exibida por padrão na guia Conhecimento. É possível selecionar uma das seguintes opções:

   - **Abrir com FAQ/Pesquisa**— Exibe as seções Categoria, Pesquisa de conhecimento e Lista de documentos de conhecimento.
   - **Abrir com a ID de documento da árvore de conhecimento** — exibe a árvore de conhecimento com a ID de documento especificada no campo fornecido. Você pode retornar ao documento da árvore de conhecimento e depois para os painéis Categoria, Pesquisa de conhecimento e Lista de documentos de conhecimento.

   Padrão: abrir com Perguntas frequentes/Pesquisa

Exibição de categoria

Especifica o formato em que as categorias de documentos são exibidas no painel Categorias de conhecimento na guia Administração. É possível selecionar uma das seguintes opções:

- Exibir categorias na exibição em árvore—Apresenta as categorias em uma estrutura de árvore hierárquica na seção Categoria de conhecimento. As categorias são expandidas para revelar subcategorias associadas. Assim, você pode exibir todas as categorias na árvore simultaneamente.
- Exibir categorias na exibição em lista—Apresenta as categorias em formato de lista na seção Categoria de conhecimento. Quando você seleciona uma categoria, suas subcategorias são exibidas em uma lista. Você só pode exibir o nível atual de categorias ou subcategorias de cada vez. Use o link Subir um nível para retornar ao nível de categoria anterior.

Observação: se você tiver mais de 250 categorias abaixo da categoria topo, ou abaixo de qualquer categoria, use Exibir categorias na opção Exibição da lista, e não a exibição em árvore.

Principais soluções

Especifica o número de documentos que devem ser listados em Soluções principais na página inicial do CA SDM.

Padrão: 10

Incluir dados globais

Exibe dados de todos os inquilinos nas Principais soluções.

Padrão: ativado

Notificações de indexação de documento

Define um usuário para receber notificações de email sobre status ou quando ocorrem erros durante a indexação de documentos. O usuário deve ter um endereço de email na tabela de ca_contacts para receber as notificações de email. Use a Página Notificação do registro de contato do responsável para definir métodos de notificação.

Importante: É fundamental definir um Responsável para receber notificações de indexação de documento na seção Notificações de Indexação de Documento. Um endereço de email deve ser definido para este destinatário na página Notificação de Contatos para ativar as notificações de email.

Clique em OK.

As configurações gerais são definidas.

Capítulo 21: Administrando o Support Automation

Esta seção contém os seguintes tópicos:

Automatizando o suporte em seu ambiente (na página 1043)
Administração do analista do Support Automation (na página 1047)
Administração do usuário do Support Automation (na página 1053)
Administração de notificação da atividade do Support Automation (na página 1058)
Adaptações da página do Support Automation (na página 1059)
Propriedades do sistema Support Automation (na página 1062)
Administração de fila no Support Automation (na página 1062)
Gerenciamento de modelo de ticket (na página 1065)
Configurações de administração (na página 1066)
Como personalizar as ferramentas do Support Automation (na página 1068)
Administração do log da sessão (na página 1076)
Relatórios do Support Automation (na página 1077)
Resolver tickets usando a assistência online (na página 1077)

Automatizando o suporte em seu ambiente

É possível implementar uma estratégia de suporte usando uma combinação de processos e ferramentas. O CA SDM fornece as ferramentas para administrar a assistência online, desenvolver tarefas automatizadas e para entregá-las por meio de vários canais de suporte.

Use os processos associados para criar e manter um ambiente que faça o seguinte:

- Reduza a média da duração da chamada de suporte
- Reduza os custos gerais de suporte
- Aumente as taxas de resolução
- Oferece maior satisfação do cliente

Assistência online

A Assistência online fornece suporte ao usuário final por meio do uso de ferramentas que aprimoram a interação remota entre analistas e usuários finais. É possível usar respostas automatizadas predefinidas para comunicar-se com o usuário final. Você obtém informações detalhadas sobre o computador de usuário final e toma providências para fornecer suporte.

Você fornece assistência online usando as seguintes interfaces:

Interface do analista do Support Automation

Permite que o analista interaja com usuários finais e forneça suporte durante sessões de assistência.

Cliente de usuário final

Permite que o usuário final converse com o analista, enquanto o analista fornece suporte a seu computador.

Conectividade do Support Automation

O analista e o usuário final nunca se comunicam diretamente entre si. Não é necessária a conectividade direta ponto a ponto entre os dois usuários. Todas as transferências de dados são roteadas através do servidor, verificando se é possível se comunicar mesmo quando o computador do usuário final está protegido por firewalls restritivos.

É possível conectar os computadores dos usuários finais usando as seguintes conexões:

Soquete

Utilizar uma conexão de soquete é a melhor maneira de realizar a conexão. As conexões de soquete são o tipo mais rápido, com menos despesas gerais, latência mínima e tipos mais eficientes de conexão.

HTTP (ou HTTPS)

Usar a conexão HTTP pode resultar em conexões melhores do que as conexões diretas por soquete, pois os firewalls corporativos podem bloquear as conexões diretas por soquete. As conexões HTTP geram uma quantidade considerável de despesas gerais de tráfego de rede em comparação às conexões diretas por soquete. Devido às despesas gerais e ao processamento do HTTP no servidor, o número de sessões simultâneas é muito menor quando a maioria das conexões com o servidor são HTTP.

Proxy

O Proxy de soquete é um modo de operação para o servidor do Support Automation para redirecionar algumas das operações intensas do CPU. Por exemplo, criptografia/descriptografia do servidor principal e para fornecer ao componente do servidor que possa ir no DMZ (ou zona semelhante) na topologia de rede lógica.

Normalmente, você tenta se conectar através da conexão direta por soquete primeiro e, então se conecta através do HTTP caso a conexão direta por soquete falhe. Entretanto, é possível especificar as configurações de conexão personalizadas no computador do cliente para alterar essa sequência.

Observação: para obter detalhes sobre a configuração de comunicação, consulte a *Ajuda on-line.*

Cliente de usuário final

O cliente do usuário final conecta os usuários finais aos analistas em sessões de assistência online. Os usuários conversam com analistas no WebChat, mas caso seja necessário usar as ferramentas na Interface com o analista do Support Automation, o CA SDM executa o cliente no computador do usuário final. Quando o cliente é iniciado, são exibidas instruções ao usuário final específicas ao seu navegador.

Carga do servidor

Em grandes implementações, altas cargas do servidor podem prejudicar o desempenho do aplicativo. Por essa razão, é possível descarregar alguns processamentos para um ou mais servidores Proxy de soquete da seguinte maneira:

- Criptografia e a descriptografia de descarga dos dados enviados e recebidos para todos os analistas ou clientes (conexão através de Soquete direto ou HTTP).
- Processamento de descarga do tráfego HTTP de e para os clientes se conectando através do HTTP ao Proxy de soquete.

Componente do servidor DMZ

Em alguns ambientes de rede, caso você autorize o acesso direto por soquete aos servidores de aplicativo sendo executados no aplicativo do servidor Support Automation, isso pode ser considerado um risco de segurança. Nesses ambientes, é possível usar o Proxy de soquete no DMZ para fornecer um componente intermediário entre os usuários de internet e os servidores de aplicativo. Usar o Proxy de soquete nesse cenário descarrega uma parte do processamento do servidor principal.

Como o proxy de soquete funciona

O Proxy de soquete funciona da seguinte maneira:

1. Na porta externa configurada, o Proxy de soquete ouve as conexões recebidas dos analistas e usuários finais.
2. O Proxy de soquete estabelece uma conexão de ponto com o Servidor principal na porta interna configurada, para cada conexão. Essas duas conexões são chamadas de conexão do usuário final e conexão do servidor, respectivamente.
3. As conexões do usuário final são criptografadas e o Proxy de soquete criptografa/descriptografa quaisquer dados recebidos ou enviados através da conexão do usuário final.

   Observação: as conexões do servidor não são criptografadas.
4. Para cada pacote de dados recebido, a estrutura do protocolo é verificada e um valor de checksum é validado antes de os dados serem passados para o servidor principal através da conexão com o servidor.
5. O servidor principal descarrega o processamento de criptografia e descriptografia.
6. O Proxy de soquete fecha a conexão de ponto correspondente assim que a conexão do usuário final ou do servidor for fechada.

Administração do analista do Support Automation

O analista do Support Automation monitora e gerencia várias solicitações de usuário final em sessões de assistência online em seu ambiente. Analistas usam ferramentas do Support Automation para interagir com usuários finais e fornecer assistência online.

Os analistas acessam a interface de um ticket do CA SDM, como um incidente, ou a guia do Support Automation. É possível gerenciar níveis de acesso para definir permissões para ferramentas que os analistas podem usar. É possível ativar e desativar ferramentas do Support Automation para inquilinos específicos. Se uma ferramenta for desativada para um inquilino, os analistas não poderão usar aquela ferramenta em sessões de assistência.

Importante: A interface do Analista do Support Automation só é executada no Windows. Para obter mais informações sobre sistemas operacionais suportados, consulte *Notas da versão*.

Mais informações:

Como os analistas iniciam a assistência online (na página 1048)
Como configurar a Assistência online para os analistas (na página 1049)
Como os usuários finais entram em sessões de assistência (na página 1050)
Como os analistas automatizam o suporte a usuários finais (na página 1052)
Como os analistas oferecem a assistência online (na página 1052)

Como os analistas iniciam a assistência online

Os analistas iniciam a Assistência online da seguinte maneira:

1. O analista realiza *uma* das seguintes ações:
   - Efetua o logon no CA SDM e seleciona a guia Automação de suporte.
   - Abre um ticket no CA SDM e seleciona a guia Automação de suporte.
2. O CA SDM solicita que o analista instale o JRE (Java Runtime Environment) de 32 bits, versão 1.6 ou posterior, caso não esteja instalado. A Interface do analista do Support Automation não oferece suporte a JRE de 64 bits.

   Observação: o navegador Safari requer o JRE de 32 bits 1.6.0_30 ou posterior.

   O CA SDM inicia a interface do Support Automation.

Observação: a tabela de sa_login_session cria um registro sempre que um analista inicia a Interface do analista da automatação de suporte e quando o usuário final inicia o cliente web. Para obter informações sobre a tabela sa_login_session, consulte o *Guia de Referência Técnica* do *CA SDM*.

Configurar as opções de conexão Java

É possível configurar as opções de conexão Java para resolver uma ocorrência em que a Interface do analista do Support Automation não pode se conectar ao servidor Support Automation. Essa ocorrência acontece quando a configuração o navegador padrão do analista não é definida de maneira adequada para seu ambiente e falha ao iniciar a Assistência online. É possível editar as configurações de conexão do analista a partir de um navegador ou do Painel de controle Java.

Para configurar as opções de conexão em seu navegador

1. Abra um navegador de web, como o Internet Explorer.

   O navegador é exibido.
2. Clique em Ferramentas, Opções da Internet.

   A caixa de diálogo Opções da Internet aparece.
3. Configure as definições de conexão adequadas, como uma conexão direta ou servidor proxy.
4. Clique em OK.

   As aberturas de conexão são configuradas.

Para configurar as opções de conexão no Painel de controle Java.

1. Abra o Painel de controle Java com o seguinte comando:

   ```
   javaws -viewer
   ```

   O Painel de controle Java é exibido.

2. Na guia Geral, clique em Configurações de rede.

   A caixa de diálogo Configurações de rede é exibida.

3. Configure as definições adequadas, como uma conexão direta ou servidor proxy.

   Clique em OK.

   As aberturas de conexão são configuradas.

Como configurar a Assistência online para os analistas

Configure a Interface do analista do Support Automation ao definir permissões de função e segurança em seu ambiente de assistência online da seguinte maneira:

1. Crie ou modifique as funções (na página 1054) e os Níveis de acesso do Support Automation (na página 1057) adequados para os analistas em seu ambiente de assistência online.

   Atualize as funções e os Níveis de acesso para oferecer aos analistas a permissão para ferramentas específicas que podem ser usadas nas sessões de assistência.

2. Estabelecer e gerenciar as filas (na página 1062) para seu ambiente de assistência online.

   Crie filas para rotear adequadamente as solicitações de assistência online recebidas.

3. Estabelecer e gerenciar as notificações de atividade (na página 1058) para seu ambiente de assistência online.

   Crie notificações de email para alertar os analistas quando tentarem obter uma solicitação de sessão de assistência em sua fila.

4. Estabelecer e gerenciar as predefinições de bate papo (na página 1075) para seu ambiente de assistência online.

   Crie pré-configurações que o analista usa para enviar as respostas pré-configuradas para as situações e perguntas comuns.

5. Estabelecer e gerenciar as tarefas automatizadas para seu ambiente de assistência online.

   Crie tarefas automatizadas para executar ações específicas no computador do usuário final.

   Observação: é possível apenas criar scripts e fazer o upload deles para o servidor através do Automated Task Editor IDE.

Como os usuários finais entram em sessões de assistência

Um usuário final solicita sessões de assistência a partir de sua página principal do CA SDM ou contatando diretamente a central de serviços, como por telefone ou email. O analista do Support Automation convida o usuário final para uma sessão a partir do ticket do CA SDM.

1. O usuário final realiza *qualquer uma* das ações abaixo:

   - Solicita um bate-papo online a partir da página principal do CA SDM.

     A página Abertura do bate-papo online é exibida perguntando ao usuário final a área e a descrição do incidente. O usuário final clica em Continuar, a sessão é aberta e o usuário final é colocado na fila adequada.

- Clica em um link de uma notificação de email e efetua o logon na sessão de assistência usando suas credenciais e um código de entrada na sessão fornecido pelo analista.

  Se o usuário final entrar a partir da notificação de email, ele ignora a fila.

- Clica em Incluir analista agora e fornece o código de inclusão de sessão para ignorar a fila.

  Observação: quando o cliente do usuário final do Support Automation for iniciado, um arquivo executável é transferido por download para iniciar o programa. O usuário final o inicia manualmente, embora, por razões de segurança, haja um tempo limitado para iniciar o executável. Após o tempo expirar, uma mensagem de erro é exibida no computador do usuário final ao tentar iniciar o executável.

2. O analista oferece a assistência online para o usuário final através do bate-papo. O usuário final usa seu navegador web para o bate-papo com o analista ou também pode abrir o agente executável.

   Observação: se o analista não puder resolver a sessão usando o bate-papo da web, ele pode convidar o usuário final a partir da janela Analyst Session para usar todas as ferramentas disponíveis na interface do analista do Support Automation. O usuário final deve aceitar a solicitação para executar o cliente em seu computador e para o analista usar as ferramentas.

Como os analistas automatizam o suporte a usuários finais

Os analistas usam ferramentas de Assistência online para realizar as seguintes tarefas em computadores de usuários finais:

- Organizar sessões de bate-papo em tempo real
- Visualizar sistemas de arquivos
  - Criar, modificar, renomear ou excluir arquivos e diretórios
  - Copiar e transferir arquivos e pastas para o computador do usuário final
- Visualizar registros do sistema
  - Criar, editar ou excluir registros
  - Exportar ou importar valores de registro do usuário final
- Capturar telas do usuário final quando a qualidade da conexão não é suficiente para assistência por controle remoto
- Visualizar a área de trabalho do computador do usuário final
- Controlar remotamente o computador do usuário final
- Executar um programa no computador do usuário final
- Reiniciar ou encerrar o computador do usuário final
- Executar tarefas automatizadas

Observação: Para obter informações detalhadas sobre como analistas usam as ferramentas de Assistência online, consulte a *Ajuda online*.

Mais informações:

Administração de nível de acesso do Support Automation (na página 1057)

Como os analistas oferecem a assistência online

O analista oferece a assistência online aos usuários finais ao usar a Interface com o Support Automation. Os analistas tratam dos usuários finais direcionados para suas filas, gerenciam as sessões de assistência e entram em sessões para as quais possuem permissão.

1. O usuário final solicita uma sessão de assistência a partir da página inicial do CA SDM ou um ticket, como um incidente, solicitação ou ocorrência.

2. O usuário final entra em uma fila.

   Observação: se o usuário final entrar em uma sessão usando um link a partir do convite por email do analista, ele ignora a fila.

   É possível configurar as áreas de solicitação do CA SDM e as categorias de ocorrência para o roteamento da fila.

3. O analista seleciona o usuário final na fila.

4. A sessão de assistência é iniciada e o analista oferece a assistência online.

   Observação: se o analista iniciar a Interface de Analista do Support Automation a partir da guia Automatização do suporte, nenhum ticket do CA SDM é associado à sessão de assistência.

5. O analista cria um ticket ao fechar a sessão de assistência e define o status *SA-Aberto* ou *SA-Fechado*, ou transfere a sessão de assistência para outra fila.

6. O analista fecha a sessão e o usuário final recebe uma notificação por email com o Log da sessão.

Observação: para obter detalhes sobre como os analistas tratam as filas e gerenciam as sessões de assistência, consulte a *Ajuda online*.

Administração do usuário do Support Automation

Os administradores de sistema e administradores de inquilinos configuram os contatos do CA SDM, as permissões de função, níveis de acesso e níveis de privacidade para definir as permissões de usuário. A seguir estão listados os usuários que usam o Support Automation.

Administrador do sistema

Define o acesso em todo o sistema para adicionar, editar e modificar todas as funções e padrões no Support Automation na guia Administração. O administrador do sistema define os analistas e inquilinos, personaliza as propriedades do sistema Support Automation e realiza as redefinições de senha.

Administrador de inquilino

Define os direitos administrativos no nível do inquilino e não concede acesso para criar ou editar outros inquilinos ou redefinir as senhas dos usuários. O inquilino do Fornecedor de serviço determina as permissões.

Analista

Define os direitos para os usuários que oferecem assistência online aos usuários finais em seu ambiente de suporte.

Usuário final

Define os direitos para os usuários que podem solicitar assistência online dos analistas em seu ambiente de suporte, como funcionários e clientes.

Como configurar Permissões de função do Support Automation

É possível configurar funções do CA SDM para ter permissões no Support Automation. É possível definir permissões de função configurando os níveis de acesso do Support Automation para analistas e níveis de privacidade para usuários finais em seu ambiente de assistência online conforme abaixo.

1. Configure os níveis de acesso apropriados para analistas em seu ambiente de assistência online.

   Os níveis de acesso de analista são criados para gerenciar permissões de analista em seu sistema, como ativar e desativar ferramentas específicas da Interface de analista do Support Automation.

2. Configure os níveis de acesso apropriados para usuários finais em seu ambiente de assistência online.

   Os níveis de privacidade são criados para gerenciar os níveis de acesso dos usuários finais em seu sistema.

3. Atribua (na página 1058) níveis de acesso a funções.

   Você atribui os níveis de privacidade de usuários finais e os níveis de acesso de analistas a funções em seu ambiente.

Observação: Para obter informações detalhadas sobre a criação e modificação de níveis de acesso para analistas do Support Automation e configuração de níveis de segurança para usuários finais, consulte a *Ajuda online*.

Usuários registrados e anônimos do Support Automation

O servidor Support Automation aceita usuários anônimos e registrados, dependendo das permissões do CA SDM. Caso seja permitido, o usuário convidado permite quem os usuários anônimos efetuem o logon no CA SDM. É possível se autenticar com o servidor para obter acesso ao seguinte:

- Assistência online
- Autoatendimento
- Editor de tarefas automatizadas
- Cliente de usuário final

Como configurar o Support Automation para Usuários convidados

É possível configurar seu ambiente de assistência online para permitir usuários convidados. Configure os usuários convidados para inquilinos específicos ou disponibilize-os para todo o sistema da seguinte maneira:

1. Crie um tipo de acesso que permite a autenticação da web (na página 1055).

   Selecione o Tipo de validação "Aberto - Sempre permitir acesso".

2. Atribua (na página 1056) o Tipo de acesso a um contato.

   É possível criar um contato convidado para os diferentes inquilinos em seu ambiente.

3. Notifique os usuários adequados em seu ambiente sobre o logon anônimo usando o seguinte formato de URL:

   http://*hostname*?USRNAME=*UserName*

Crie um tipo de acesso para os usuários convidados

É possível criar um tipo de acesso que permita que os usuários convidados efetuem o logon no CA SDM sem a autenticação. Caso você seja o fornecedor de serviço, pode criar um tipo de acesso para cada inquilino em seu ambiente.

Para criar um tipo de acesso de convidado

1. Clique em Gerenciamento de segurança e função, Tipos de acesso.

   É exibida a Lista de tipos de acesso.

2. Clique em Criar novo.

   A página Criar tipo de acesso aparece.

3. Preencha os campos conforme apropriado, como símbolo e descrição.
4. Na guia Autenticação da web, selecione *Aberto - Sempre permitir acesso* na lista suspensa Tipo de validação.
5. Salve o tipo de acesso.

   O tipo de acesso é criado.
6. (Opcional) Clique com o botão direito do mouse na página Lista de tipo de acesso para atualizar essa página de lista.

   O tipo de acesso de convidado é exibido na lista.

Atribua o Tipo de acesso de convidado a um contato.

É possível atribuir o tipo de acesso de convidado a um contato após criar um tipo de acesso que usa a autenticação de web para que o contato possa efetuar o logon no CA SDM. É possível notificar os usuários adequados em seu ambiente sobre o contato convidado após atribuir o tipo de acesso.

Para atribuir o tipo de acesso de convidado

1. Clique em Gerenciamento de segurança e função, Contatos.

   A página Pesquisa de contato aparece.
2. Clique em Criar novo.

   A página Criar contato aparece.

   Observação: é possível também modificar um contato.
3. Selecione convidado na lista suspensa Tipo de contato.
4. (Opcional) Associe o contato a um inquilino. É possível também tornar um contato público.
5. Salve o contato.

   O contato é criado e o tipo de acesso de convidado é associado ao contato.

Administração de nível de acesso do Support Automation

É possível gerenciar os níveis de acesso do Support Automation e atribuí-los às funções do CA SDM em seu ambiente de suporte. Os ambientes de suporte variam em tamanho e estrutura, então a implementação dos níveis de acesso pode variar.

Em um ambiente de suporte pequeno, é possível haver um ou dois analistas categorizados em um único nível de acesso, como Analista. Em um ambiente de suporte maior, o administrador de inquilino pode definir muitos níveis de acesso de analista, cada um deles com privilégios de suporte e acesso diferentes.

Importante: Caso esteja em um ambiente de multilocação, os analistas que não pertencem ao provedor de serviço podem gravar o acesso apenas para seus próprios inquilinos ou subinquilinos. É possível fornecer o acesso à gravação de analista para os outros inquilinos e subinquilinos ao atualizar o acesso de função do inquilino acessado para incluir inquilinos que não sejam fornecedores de serviços.

Os seguintes níveis de acesso estão disponíveis:

Analista

Especifica o tipo de contato que oferece assistência online aos usuários finais em seu ambiente de suporte. Os níveis de acesso definem quais filas, tarefas automatizadas e ferramentas estão disponíveis para uso pelo analista.

Usuário final

Especifica o tipo de contato que recebe a assistência online dos analistas, como funcionário e cliente.

É possível gerenciar os níveis de acesso do Support Automation a partir da guia Administração.

Observação: para obter informações detalhadas sobre como criar e modificar os níveis de acesso do Support Automation para os analistas e usuários finais, consulte a *Ajuda online*.

Atribua o Nível de acesso a uma função

É possível gerenciar os níveis de acesso do Support Automation às funções existentes do CA SDM em seu ambiente.

Para atribuir um nível de acesso a uma função

1. Selecione Gerenciamento da segurança e funções, Gerenciamento de funções, Lista de funções na guia Administração.

   A página Lista de funções aparece.

2. Clique na função à qual deseja atribuir o nível de acesso, como Administrador.

   A página Detalhes da função aparece.

3. Clique em Editar.

   A página Atualizar função aparece.

4. Na guia Autorização, selecione o nível de acesso criado a partir da lista suspensa Acesso à automação de suporte e clique em Salvar.

   A página Detalhes da função aparece. Verifique se o acesso do Support Automation foi atribuído à função.

Administração de notificação da atividade do Support Automation

É possível usar as notificações de atividade para gerenciar as atividades do Support Automation. É possível também personalizar como os usuários finais e administradores rastreiam e recebem as notificações quando uma atividade ocorre, por exemplo, o término da sessão de uma assistência .

Configure qualquer uma das notificações padrão a seguir, conforme apropriado para seu ambiente:

Notificação de entrada na fila

Notifica o analista quando um usuário final entra em uma fila de sessão de assistência.

Notifica o analista quando uma sessão de assistência é transferida para outra fila.

Notificação do analista

Notifica o analista quando o tempo de espera da fila do usuário final expira. O evento de expiração é reconhecido com a macro Condicional de evento do CA SDM.

Convidar o usuário final para uma sessão de assistência - incidente

Notifica o usuário final quando o analista o convida para uma sessão de assistência a partir de um incidente ou solicitação.

Convidar o usuário final para uma sessão de assistência - ocorrência

Notifica o usuário final quando o analista o convida para uma sessão de assistência a partir de uma ocorrência.

Notificação de término da sessão

Notifica o sistema quando a sessão de assistência termina.

Importante: Caso deseje usar a funcionalidade do Support Automation com um sistema externo, como o Star, o contato System_SA_User é definido, por padrão, com a regra *Notificação de término da sessão*.

Adaptações da página do Support Automation

É possível configurar a aparência das páginas do Support Automation para seus usuários finais de acordo com suas necessidades de negócios. As adaptações a seguir permitem que você controle o que o usuário vê antes de entrar na sessão de assistência e após a sessão ser concluída:

- Personalizar o cabeçalho e o rodapé de todas as páginas que o usuário final vê.

  É possível alterar o código HTML do cabeçalho e do rodapé, além de modificar o local do arquivo CSS que contém as definições de estilo.

- Personalizar as necessidades de localização de seu ambiente.

  É possível definir o local padrão para todos os analistas e usuários finais.

- Personalizar os layouts de páginas que os usuários finais veem ao efetuar o logon para entrar nas sessões de assistência.

  É possível personalizar as páginas que direcionam seus usuários finais para atender as necessidades de negócios.

Observação: para obter detalhes sobre como configurar as páginas do Support Automation para os analistas e usuários finais, consulte a *Ajuda online*.

Administração de marca

É possível personalizar o cabeçalho e o rodapé das páginas direcionadas a um usuário final como um autoatendimento. É possível alterar o código HTML do cabeçalho e do rodapé, além de modificar o local do arquivo CSS que contém as definições de estilo.

É possível visualizar uma lista dos registros de marca, um para cada inquilino no máximo. Os inquilinos podem criar sua própria marca ou, se a marca não estiver definida para o inquilino, ele utilizará as configurações padrão do sistema. É possível ainda permitir a localização da marca e visualizar uma lista de todas as marcas localizadas par aos locais ativos.

Importante: As personalizações de marca do CA Support Automation r.6.0 SR1 eFix5 não migram para o CA SDM Release 12.7 automaticamente. Recomendamos que você analise a marca personalizada para verificar se correspondente à marca do CA SDM. Se necessário, copie e cole o Cabeçalho, Rodapé e dados do URL da CSS de cada divisão para o respectivo inquilino (ou público) no CA SDM para migrar os dados de marca.

Administração de localização

A localização permite o suporte a vários idiomas simultaneamente na mesma instalação, traduzindo elementos do aplicativo a um idioma em particular. Esses elementos podem incluir mensagens de sistema, ícones e conteúdo. As informações são apresentadas na melhor forma para o usuário final, não importa seu idioma nativo.

Versões localizadas do Support Automation atendem às necessidades de seu ambiente global. Cada inquilino pode receber vários idiomas, e as localizações são suportadas para vários inquilinos. Cada inquilino compartilha as configurações padrão do sistema com sua localização. É possível configurar o idioma que o usuário final e o analista usarão antes de iniciar a Assistência online a partir da lista de idiomas ativados. O analista pode usar um idioma diferente daquele do analista em uma sessão de assistência.

É possível editar texto localizado para isenções de responsabilidade. Não é possível criar ou remover localizações, mas é possível ativá-las ou desativá-las.

Observação: a interface do administrador está disponível somente na localização padrão do servidor.

Configuração de layout de página

Quando usuários finais fazem logon na Assistência online a partir do CA SDM, é exibida a página inicial padrão. Da mesma forma, quando são colocados em espera em uma fila, veem novamente uma página padrão.

Se nenhuma configuração especial for especificada para inquilinos, eles utilizam configurações públicas. É possível configurar os seguintes parâmetros públicos para filas que não têm suas próprias definições especializadas:

- Página de espera
- Página de pós-início do usuário final
- Em sessão
- Página pós-logoff
- Sair da página de pesquisa

Cada página tem sua própria página de detalhe, que compreende um campo de texto para inserir o URL e uma caixa de seleção para marcar esta página como externa.

Propriedades do sistema Support Automation

Você pode personalizar muitas das formas em que o Support Automation manipula as atividades para diferir da instalação padrão. É possível usar as configurações de opção do sistema padrão para personalizar o comportamento do Support Automation. Por exemplo, é possível personalizar as seguintes opções do Support Automation:

- Ative ou desative o link para o bate-papo online da página inicial dos clientes e funcionários do CA SDM.
- Ative ou desative o link para Entrar em uma sessão da página inicial dos clientes e funcionários do CA SDM.
- Ative ou desative a opção para criar um incidente do CA SDM quando o usuário final desconectar enquanto aguarda para ser atendido em uma fila de Support Automation.

As propriedades do sistema são opcionais quanto ao inquilino. Se um inquilino não definiu suas propriedades, o Support Automation usa as configurações públicas (compartilhadas). A instalação do produto cria propriedades públicas padrão.

Observação: para obter mais informações sobre a configuração das propriedades do sistema Support Automation, consulte a *Ajuda online*.

Administração de fila no Support Automation

As filas são usadas para rotear as solicitações de sessão de assistência para o analista mais adequado. O usuário final pode selecionar uma categoria ou inserir uma descrição do problema de seu computador e seu ticket (como um incidente) é roteado para a fila adequada.

Após a instalação inicial do produto, a fila padrão é chamada de Suporte. É possível definir diversas filas para facilitar a classificação e o rastreamento de diferentes solicitações de suporte, de acordo com suas necessidades de negócios. É possível atribuir apenas uma fila padrão por inquilino. Caso um padrão não seja atribuído a uma fila de inquilino ou se a fila padrão de inquilino estiver indisponível, o sistema usa a fila pública padrão. As horas de trabalho são definidas por fila.

O sistema determina automaticamente onde colocar o usuário final ao mapear as filas por áreas de incidentes. Se uma área mapear para uma rede, o usuário final seleciona uma categoria e é roteado para a fila adequada. Os recursos de pesquisa são aplicados à descrição de uma categoria de ocorrência ou incidente para identificar as filas relevantes e o usuário final é roteado apenas para a fila com melhor correspondência.

Observação: para obter informações mais detalhadas sobre a personalização e o mapeamento das filas Support Automation, consulte a *Ajuda online*.

Gerenciamento de fila

As filas são configuradas para ajudar os usuários finais a receberem a assistência online adequada dos analistas. As filas são gerenciadas para melhorar a maneira que os usuários finais são roteados para as sessões de assistência da seguinte maneira:

- Personalizar as filas para os analistas e inquilinos em seu ambiente de assistência online.

  É possível ativar ou desativar as filas e especificar as permissões dos inquilinos e analistas.

- Atribuir uma fila padrão.

  Você pode encaminhar os usuários finais à fila padrão quando eles digitam consultas que não correspondem às filas configuradas em seu ambiente. É possível também personalizar as filas para os inquilinos em seu ambiente.

  Observação: se a fila de inquilino padrão estiver ausente ou indisponível, a fila pública é usada.

- Atribuir horário de operação para suas filas.

  É possível gerenciar as filas com base na disponibilidade dos usuários em seu ambiente de suporte, como ativar os serviços do Support Automation durante o horário comercial.

  Importante: Você pode atribuir turnos de trabalho tanto a suas horas de Support Automation como a filas de assistência online individuais. Diferentes turnos de trabalho atribuídos a horas do Support Automation e filas individuais podem causar conflitos para analistas e usuários finais em seu ambiente de suporte.

Como gerenciar resumos de fila

É possível compor os campos que um analista visualiza na página Queue Summaries. É possível selecionar a partir do seguinte grupo de campos para o resumo de fila, mas não é possível criar campos:

- Fila
- Pergunta
- Tempo de espera
- Email
- Empresa
- Endereço IP
- Analista proprietário
- Categoria
- Idioma
- Inquilino

Mais informações:

Gerenciamento de fila (na página 1063)
Como gerenciar as horas da fila (na página 1065)

Como gerenciar as horas da fila

É possível ativar o Support Automation para cada fila para horas específicas do dia, para abrigar o horário de trabalho dos analistas da seguinte maneira:

- Crie uma programação separada para cada fila e para todos os serviços de suporte automatizados.

  Observação: essas configurações não se limitam a funções de autoatendimento.

- Define as horas de suporte para o servidor através de um status global de aberto ou fechado. Uma entrada para cada hora da semana indica uma diferença do status global do servidor.
- O servidor usa a primeira entrada para cada hora com base nas regras estabelecidas.

  Essa ação efetivamente mescla as definições de hora de suporte das configurações do inquilino pai (ou público). Essa ação pode ter resultados nada lógicos caso um misto de 'padrão-fechado' e 'padrão-aberto' seja usado na hierarquia.

Gerenciamento de modelo de ticket

É possível especificar que modelos de ticket de estão disponíveis para a interface de usuário do analista. Você pode selecionar os modelos de ticket para os tipos de ticket de Incidentes/Solicitações e Ocorrência.

Você pode definir se o modelo é padrão ou ativo. Ao criar um modelo de ticket, você pode selecionar dentre os modelos existentes do CA SDM. O modelo padrão deve estar ativo.

Você pode ter apenas um modelo de ticket como padrão por inquilino.

Observação: para obter informações mais detalhadas sobre a personalização dos modelos de ticket, consulte a *Ajuda online*.

Configurações de administração

É possível definir e configurar as seguintes definições do Support Automation:

- Servidores de roteamento de mensagem
- Permissões do usuário final (Níveis de privacidade)
- Horas do Support Automation

Como definir as Configurações do Support Automation

É possível definir as configurações do Support Automation para seu ambiente de suporte de acordo com suas necessidades de negócios. As configurações permitem que você controle a funcionalidade administrativa, como servidores de roteamento de mensagem, níveis de privacidade de horas do Support Automation.

- Configure os servidores de roteamento de mensagem para melhorar o desempenho durante a sessão de assistência.

  É possível conectar os usuários finais ao servidor local preferido do analista ou, se a conexão não for bem sucedida, conectar a sessão ao servidor padrão principal.

- Define os níveis de privacidade para os usuários finais em seu ambiente.

  É possível ativar ferramentas da Interface do analista do Support Automation específicas, com base nos níveis de privacidade usados em seu ambiente.

- Defina suas horas do Support Automation para horas específicas de operação ou como aberto o tempo todo.

  É possível direcionar as solicitações de assistência online quando a central de suporte estiver fechada, como abrindo uma página da web informando ao usuário final sobre os horários da central de suporte e opções de suporte adicionais.

Observação: para obter mais informações sobre a definição das configurações do Support Automation, consulte a *Ajuda online*.

Servidores de roteamento de mensagem

Você pode usar os Servidores de roteamento de mensagem (MRS) para gerenciar vários servidores de Controle remoto, com base na localização geográfica do servidor local. Usar os MRS ajuda a melhorar o desempenho durante sessões de assistência. Ao ativar o MRS, a Interface do analista do Support Automation e o cliente do usuário final tentam se conectar ao servidor (local) preferido do analista para o compartilhamento. Se a conexão for malsucedida, a sessão de compartilhamento retorna ao servidor padrão principal. O Log ao vivo registra quais MRS você usa durante a sessão de assistência.

Crie, atualize, remova, ative ou desative um objeto de servidor de roteamento de mensagem.

Observação: para obter mais informações sobre a configuração dos servidores de roteamento de mensagem, consulte a *Ajuda online*.

Níveis de privacidade de Support Automation

Os níveis de privacidade são usados para definir quais ações são permitidas para serem realizadas em diferentes usuários finais para proteger a privacidade do usuário. Os níveis de privacidade estão associados às funções do CA SDM. Existem três permissões padrão: Alta, Média e Baixa, mas podem ser definidas outras, se necessário. Você pode adicionar, atualizar e excluir níveis de privacidade que estão à disposição do usuário final.

Você pode definir o nome do nível de privacidade e sua descrição. É possível definir quais funções para as ferramentas especificadas (Gerenciador de arquivos, Registro remoto, Executar programa, etc) estão ativadas para esse nível de privacidade.

Observação: para obter mais informações sobre a configuração dos níveis de privacidade do Support Automation, consulte a *Ajuda online*.

Horas do Support Automation

Você pode definir o Support Automation para operar em horários específicos ou para operar em todas as ocasiões. Você gerencia estas horas de operação com base nas necessidades dos usuários finais em seu ambiente de suporte. Os usuários finais não podem acessar a funcionalidade do Support Automation quando ele está fechado. Você pode fazer rápidas mudanças em vários turnos de trabalho em uma única etapa.

Importante: Você pode atribuir turnos de trabalho tanto a suas horas de Support Automation como a filas de assistência online individuais. Diferentes turnos de trabalho que são atribuídos a horas do Support Automation e filas individuais podem causar conflitos para analistas e usuários finais em seu ambiente de suporte.

Observação: para obter mais informações sobre a configuração das horas do Support Automation, consulte a *Ajuda online*.

Como personalizar as ferramentas do Support Automation

É possível configurar as ferramentas do Support Automation para seu ambiente de suporte de acordo com suas necessidades de negócios. As configurações permitem que você controle a funcionalidade administrativa, como tarefas automatizadas, predefinições de bate-papo, credenciais padrão e Declarações de isenção de responsabilidade.

- Personalize a lista de tarefas automatizadas e as classificações que os analistas Support Automation usam para fornecer suporte a usuários finais.
- Configure predefinições de bate-papo para as respostas comuns para as situações perguntas comuns.
- Configure as credenciais padrão que permitem obter acesso ao computador do usuário final.
- Personalize as declarações de isenção de responsabilidade que os usuários veem antes de executar as tarefas de autoatendimento.

Observação: para obter mais informações sobre a configuração das ferramentas do Support Automation, consulte a *Ajuda online*.

Tarefas automatizadas

Uma *tarefa automatizada* é uma coleção de etapas que definem um processo automatizado que o analista ou usuário final segue. Etapas de tarefas automatizadas são rotinas escritas em VBScript ou JavaScript que realizam ações específicas no computador do analista ou do usuário final. É possível criar novas tarefas e etapas de tarefas automatizadas usando o Editor de tarefas automatizadas. As rotinas comuns incluem reunião de informações de telemetria, diagnóstico de problemas e implementação de resoluções.

Ao executar uma tarefa automatizada, o log é atualizado. Este log é vinculado e acessado pelo log da sessão de assistência. Entradas no log de tarefas automatizadas consistem em uma série de entradas de texto com carimbos de data e hora.. As entradas são criadas com chamadas para Functions.LogMessage() ou WScript.Echo().

Mais informações:

Como implementar tarefas automatizadas (na página 1070)

Como configurar tarefas automatizadas

Instale e configure o Editor de tarefa automatizada para gerenciar as tarefas automatizadas que os analistas Support Automation usam para oferecer suporte aos usuários finais. O usuário pode executar uma tarefa automatizada a partir de um documento de conhecimento e da interface de autoatendimento, ou um analista executa uma tarefa automatizada durante uma sessão de assistência. As tarefas automatizadas fornecem aos analistas informações detalhadas sobre o computador de um usuário final. Crie tarefas automatizadas de autoatendimento que interajam com o usuário final e processem sua entrada. Essas tarefas podem alterar o sistema de arquivo, registro, download de software de instalação, etc. Configure as tarefas automatizadas da seguinte maneira:

1. Instale o Editor de tarefas automatizadas.

   Excute o instalador a partir do seguinte local na mídia de instalação:

   ```
   casd.nt\SAScriptWriter
   ```

   Observação: é possível também copiar o instalador e implementá-lo para os usuários apropriados em seu ambiente de suporte.

   O Editor de tarefas automatizadas é instalado.

2. Abra o Editor de tarefas automatizadas.

   A instalação do Editor de tarefas automatizadas cria um atalho em sua área de trabalho.

3. Defina os seguintes parâmetros de conexão:

   a. Clique em Ferramentas, Servidor.

      A caixa de diálogo Configuração do servidor é exibida.

   b. Insira o nome do host e a porta.

      Porta padrão: 8070

   c. Insira o nome de usuário e a senha de um usuário com direito de leitura/gravação para o Editor de tarefas automatizadas, como um Analista do Support Automation.

   d. Clique em Testar.

   e. Clique em OK.

4. Crie tarefas automatizadas e faça o upload delas ao seu servidor.

   É possível efetuar o upload de tarefas públicas ou atribuí-las a inquilinos e subinquilinos específicos.

   Importante: Apenas funções do inquilino do Provedor de serviço com o sinalizador Atualizar público ativado podem fazer o upload de tarefas e bibliotecas para o servidor. Todo o conteúdo da biblioteca de tarefas e o conteúdo estático são armazenados como dados públicos.

Como implementar tarefas automatizadas

É possível usar as tarefas automatizadas para ajudar os usuários finais em seu ambiente de suporte. As tarefas automatizadas realizam ações específicas sem a necessidade de o analista ou o usuário final concluir o processo. Esses scripts podem ajudar a reunir informações de telemetria, a diagnosticar problemas no computador e implementar as soluções.

Para implementar tarefas automatizadas, faça o seguinte:

1. Identifique as oportunidades de automação de suporte.

   Você encontra problemas comuns enfrentados pelos usuários finais e decide que pode automatizar algumas soluções para reduzir os custos de suporte.

2. Automação de pesquisa de soluções potenciais.

   Você procura resoluções para os problemas comuns e reúne dados sobre os processos de diagnóstico que planeja usar.

3. Projetar tarefas para automatizar o suporte ao usuário final.

   Você projeta a experiência de usuário final que deseja para cada tarefa com o Editor de tarefa automatizada.

4. Implemente e teste as tarefas automatizadas.

   Você testa as tarefas automatizadas para verificar se elas resolvem problemas comuns encontrados em seu ambiente de suporte e reduzem os custos de suporte.

5. Implemente e monitore as tarefas automatizadas.

   Você implementa as tarefas automatizadas para os usuários finais em seu ambiente ao permitir que o analista use-as nas sessões de assistência ou também é possível anexar scripts aos documentos de conhecimento.

   Importante: Se estiver em ambiente multilocação e quiser permitir que os analistas façam upload de tarefa e conteúdo de biblioteca, sua função deve ter a opção Atualizar público ativada.

Observação: o CA Technologies pode oferecer treinamento na criação de componentes e tarefas automatizadas, como bibliotecas e modelos de etapa de tarefa automatizada, que pode ser usados em seu ambiente. Para obter mais informações sobre o desenvolvimento de tarefas automatizadas, entre em contato com *Serviços CA Technologies*.

Administração de tarefas automatizadas

É possível criar tarefas automatizadas e associá-las com o servidor. Você precisa de acesso de leitura/gravação em todas as tabelas relacionadas a tarefas automatizadas para usar o Editor de tarefas automatizadas. É possível realizar funções de gerenciamento de usuários com o aplicativo, como atribuir tarefas automatizadas a funções e inquilinos.

Observação: Se você for um analista de Provedor de serviços e tiver acesso a vários inquilinos, é possível selecionar o contexto do inquilino de qualquer operação de atualização de tarefa no servidor. Também é possível atribuir uma tarefa automatizada como pública.

Implementação da tarefa automatizada

Após criar e testar uma tarefa no Editor de tarefa automatizada, é possível implementá-la para uma classificação no servidor CA SDM para ser usada nas sessões de assistência ou no autoatendimento. Algumas configurações que não fazem parte da definição da tarefa automatizada são definidas ao implementar a tarefa.

É possível fazer o download ou upload de tarefas automatizadas diretamente para o servidor a partir do Editor de tarefa automatizada. Selecione o inquilino apropriado ao criar classificações da tarefa automatizada. Caso faça o upload de scripts para o servidor, selecione a classificação ou o inquilino em que possui acesso ou defina o script como público. É possível também importar tarefas automatizadas dos arquivos XSDF e exportá-las para arquivos XSDF.

Importante: Se estiver em ambiente multilocação e quiser permitir que os analistas façam upload de tarefa e conteúdo de biblioteca, sua função deve ter a opção Atualizar público ativada.

Upload de uma tarefa automatizada

É possível fazer o upload das tarefas automatizadas criadas no aplicativo. Ao selecionar uma tarefa, todo o conteúdo dependente é automaticamente transferido por upload, como bibliotecas e conteúdo estático.

Para fazer o upload de uma tarefa automatizada

1. Abra o Editor de tarefas automatizadas.

   O Editor de tarefas do Support Automation aparece.

2. Selecione a tarefa automatizada da qual deseja fazer o upload.
3. Selecione a classificação em que deseja fazer o upload da tarefa.

   Observação: caso você seja um usuário privilegiado em um ambiente de multilocação, selecione o inquilino adequado ao fazer o upload da tarefa automatizada ou faça com que a tarefa seja pública.

4. Na barra de ferramentas, selecione o ícone Fazer upload de tarefa automatizada.

   O Editor de tarefas do Support Automation faz o upload para o servidor.

Editar uma tarefa automatizada

É possível fazer o download de tarefas automatizadas diretamente do servidor e editá-las no Editor de tarefa automatizada. Qualquer conteúdo que seja mais recente na versão do que o conteúdo existente nos servidores é importado para o banco de dados e disponibilizado para os administradores do inquilino.

Para editar uma tarefa automatizada

1. Abra o Editor de tarefas automatizadas].

   O Editor de tarefas do Support Automation aparece.

2. Na barra de ferramentas, selecione o ícone Fazer upload de tarefa automatizada.

   O Open Automated Task da seção Servidor é exibido.

3. Selecione a tarefa automatizada da qual deseja fazer download.

   Observação: caso você seja um usuário privilegiado em um ambiente de multilocação, pode editar as tarefas automatizadas específicas do inquilino ou públicas.

4. Clique em Abrir tarefa.

   O Editor de tarefa do Support Automation faz o download para o cliente e a abre no aplicativo.

   O download cria um arquivo de texto no computador do autor da tarefa que contém o conteúdo dependente.

Credenciais da tarefa automatizada

É possível executar uma tarefa automatizada para a qual você precisa de privilégios administrativos para executar, como realizar a instalação do software, ao fazer o seguinte:

- Definir as Credenciais padrão para o inquilino e configurar a tarefa automatizada para usar as credenciais padrão na administração da tarefa automatizada.
- Definir as Credenciais padrão para o inquilino e selecionar que usa a caixa de diálogo Executar como na janela Sessão de assistência.
- Definir as credenciais de tarefas automatizadas para a tarefa e especificar o uso da caixa de diálogo Executar como na janela Sessão de assistência.
- Especificar as credenciais na caixa de diálogo Executar como na janela Sessão de assistência.

Atribuição de função

Atribua as funções apropriadas (por exemplo, Analista, Administrador) para usar a tarefa automatizada. Atribua as tarefas automatizadas individuais para funções selecionadas para limitar as tarefas automatizadas para apenas esses analistas na função atribuída. É possível gerenciar os diferentes conjuntos de habilidades de experiência na organização do suporte.

É possível gerenciar as funções no nível da tarefa selecionando determinadas tarefas comumente executadas, como diagnósticos a serem executados automaticamente quando o usuário final entra em uma sessão.

Atribua o Nível de acesso a uma função

É possível gerenciar os níveis de acesso do Support Automation às funções existentes do CA SDM em seu ambiente.

Para atribuir um nível de acesso a uma função

1. Selecione Gerenciamento da segurança e funções, Gerenciamento de funções, Lista de funções na guia Administração.

   A página Lista de funções aparece.

2. Clique na função à qual deseja atribuir o nível de acesso, como Administrador.

   A página Detalhes da função aparece.

3. Clique em Editar.

   A página Atualizar função aparece.

4. Na guia Autorização, selecione o nível de acesso criado a partir da lista suspensa Acesso à automação de suporte e clique em Salvar.

   A página Detalhes da função aparece. Verifique se o acesso do Support Automation foi atribuído à função.

Administração de predefinição de bate-papo

É possível criar respostas comuns para as situações perguntas comuns. Em vez de digitar repetidamente a mesma informação, é possível salvá-la e utilizá-la em outra sessão de software.

É possível enviar as predefinições para os usuários finais no início de cada sessão automaticamente, por exemplo, uma saudação. É possível também automaticamente preencher as predefinições com informações específicas para a sessão atual, como o nome do analista.

É possível usar os seguintes tipos de predefinições em uma sessão de assistência:

Predefinição de bate-papo

Identifica uma resposta de texto normalmente usada para uma pergunta do usuário final.

Predefinição de URL

Identifica um URL texto normalmente usado que o usuário final pode acessar.

É possível localizar a predefinição do bate-papo. A predefinição de bate-papo é sincronizada com a localização do usuário final para que o usuário final receba as predefinições localizadas corretamente.

Como gerenciar as predefinições do bate-papo

É possível usar respostas predefinidas para as situações perguntas comuns.

1. Compreender as sessões de assistência típicas em sua organização.
2. Criar predefinições de bate-papo e URL com base nas necessidades de sua organização
3. Especificar se as predefinições serão disponibilizadas para inquilinos específicos ou para o público.
4. (Opcional) Duplicar a estrutura de árvore de predefinição para gerenciar ambientes localizados.
5. Enviar predefinições de bate-papo e um URL durante uma sessão de assistência.

Observação: para obter mais informações sobre a configuração das Predefinições do bate-papo, consulte *Ajuda online*.

Credenciais padrão

Você ode executar tarefas automatizadas no computador do usuário final mesmo se o usuário final não tiver direitos de acesso ao sistema para realizar essas atividades. Se o usuário final atual não tiver direitos administrativos de exibir as informações do sistema sobre seu computador, você pode executar uma tarefa automatizada restrita usando credenciais padrão para obter acesso.

Observação: para obter mais informações sobre a configuração de credenciais padrão, consulte a *Ajuda online*.

Declarações de isenção de responsabilidade

Quando os usuários finais executarem tarefas de autoatendimento, lhes são apresentados textos de declaração de isenção com os quais devem concordar antes de poderem prosseguir.

Você pode criar, atualizar e excluir os objetos comerciais de declaração de isenção.

Observação: para obter mais informações sobre a configuração das instruções do Support Automation, consulte a *Ajuda online*.

Administração do log da sessão

O log da sessão permite exibir todas as ações que os analistas realizaram durante uma sessão de assistência, assim como as ferramentas usadas e os detalhes do bate-papo (excluindo sussurros). É possível imprimir ou enviar o log da sessão por email para o usuário final. Os usuários finais também podem exibir e salvar o log, mas eles não podem modificá-lo.

Exibir o log da sessão

Todas as ações realizadas durante a sessão de assistência, como diálogo de bate-papo (excluindo conversas privadas), resultados de tarefas automatizadas e uso de uma ferramenta específica da Interface do analista do Support Automation atualizam o Log de sessão.

Para exibir o log de sessão

1. Abra a exibição da sessão ativa.

   A página Sessão ativa é exibida.

2. Selecione Log de sessão na barra de ferramentas ou no menu Sessões.

   A página Log de sessão é exibida.

3. Clique em Atualizar agora.

   A página é atualizada.

4. (Opcional) Marque a caixa de seleção Atualizar automaticamente.
5. (Opcional) Clique em Salvar log em disco.

   A caixa de diálogo Salvar é exibida. É possível salvar o log de sessão localmente como um arquivo HTML.

Relatórios do Support Automation

O CA Business Intelligence instala um conjunto de relatórios do Support Automation predefinidos. O CA SDM implementa automaticamente esses relatórios no BusinessObjects durante a instalação.

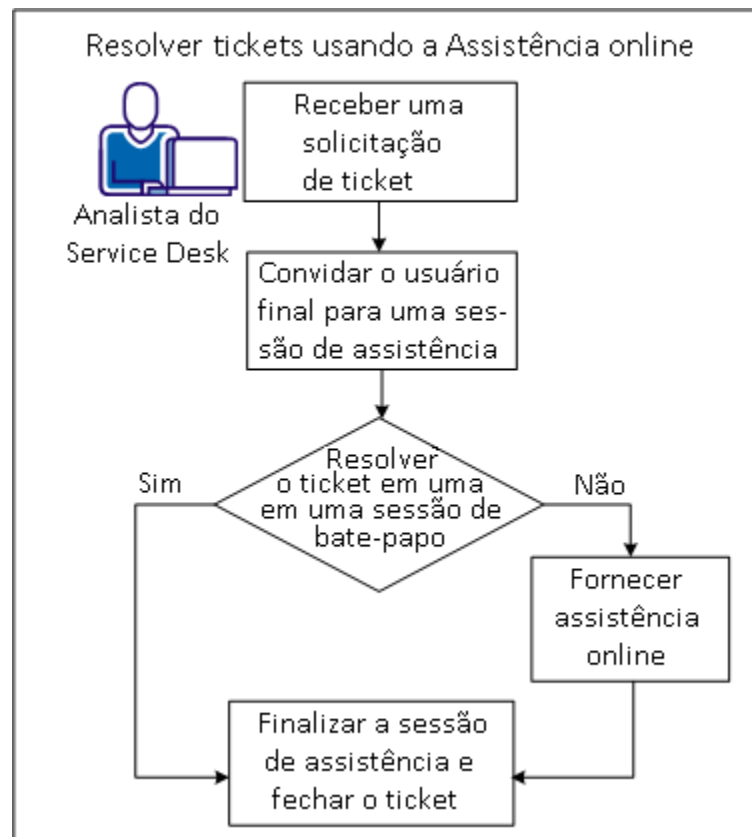
As funções de Administrador do Support Automation e Analista do Support Automation podem usar o BusinessObjects InfoView para exibir informações detalhadas e resumidas sobre o seguinte:

- Métricas de logon do analista
- Métricas de sessões de assistência
- Métricas de entradas de fila
- Métricas de execução de tarefas automatizadas
- Uso de ferramentas por categoria de ticket
- Dados em tempo real sobre usuários finais colocados em filas de suporte, sessões de assistência ativas e analistas ativos (logados).

Observação: para obter mais informações sobre como usar o BusinessObjects InfoView, consulte informações sobre o CA Business Intelligence na *Ajuda online*.

Resolver tickets usando a assistência online

Uma *sessão de assistência* permite que um Analista do Service Desk forneça assistência online aos usuários finais no CA SDM para resolver tickets. Você exibe os detalhes de um ticket do CA SDM sobre um usuário final que tem um problema no computador. Você pode bater papo com o usuário e pode convidar o usuário final para uma sessão de assistência. Use a funcionalidade de automação de suporte no CA SDM para resolver tickets usando a Assistência online. Por exemplo, o usuário final cria um ticket sobre um problema de conexão de rede com um aplicativo de software.

O diagrama a seguir explica como um Analista do Service Desk soluciona um ticket usando a Assistência online:

Execute estas etapas para fornecer assistência online para resolver um ticket do CA SDM:

1. Receber um solicitação de ticket (na página 1079).
2. Convidar o usuário final para uma sessão de assistência (na página 1079).
3. Resolva o ticket com uma sessão de bate-papo (na página 1080) ou fornecer assistência online (na página 1081).
4. Encerrar a sessão de assistência e fechar o ticket (na página 1082).

Receber um solicitação de ticket

Um usuário envia um ticket que descreve uma ocorrência em seu computador. Exibir os detalhes do ticket de um alerta por email ou do placar do CA SDM. Por exemplo, o usuário não poderá usar um aplicativo de software configurado para sincronizar com a rede.

Siga estas etapas:

1. Efetue logon no CA SDM e selecione o Placar, Minha fila.
2. Abra um ticket.
3. Revise a descrição do ticket.
4. (Opcional) Adicione um comentário no ticket que solicita que o usuário forneça mais informações sobre o aplicativo de software configurado de forma incorreta.

Convidar o usuário final para uma sessão de assistência.

Convidar o usuário para uma sessão de assistência para resolver o ticket. Por exemplo, você precisa de informações sobre as configurações de rede do computador do usuário final.

Siga estas etapas:

1. Na guia Automação de suporte da página Detalhes do ticket, clique em Convidar usuário final.
2. Digite a mensagem de saudação para o usuário final.
3. Clique em Iniciar.

   A Interface do analista do Support Automation é exibida e você deve aguardar que o usuário ingresse na sessão de assistência.

Resolver o ticket com uma sessão de bate-papo

Inicie uma sessão de bate-papo e o usuário receberá uma notificação de email do CA SDM. Este email contém um link para a sessão de assistência e os detalhes do ticket. Esse link abre o cliente do usuário final do Support Automation no computador. Inicie o bate-papo com o usuário para determinar como resolver seu ticket.

Observação: se o usuário final não puder ingressar na sessão de assistência a partir de um URL, envie um email para o usuário para clicar em Juntar-se ao analista agora na página inicial de Autoatendimento.

Siga estas etapas:

1. Clique na guia Bate-papo na interface do analista do Support Automation.
2. Execute uma das seguintes ações:
   - Selecione uma pergunta, instrução ou URL da lista suspensa Predefinições de bate-papos.
   - Digite texto na janela de bate-papo e clique em Enviar.

     Por exemplo, pergunte ao usuário final sobre as portas de rede especificadas durante a configuração do software aplicativo.
   - Envie um URL específico para o usuário final.

     O usuário final abre manualmente o link no navegador.

Fornecer assistência online

Use a Interface do analista do Support Automation para fornecer assistência online para realizar diferentes ações no computador do usuário final. Execute ações como a execução de scripts de diagnóstico, procurar o arquivo de sistema e controlar remotamente o computador do usuário final. Por exemplo, um recurso de bate-papo com o usuário determina que você pode resolver o problema de sincronização de aplicativos de software usando a Assistência online.

Siga estas etapas:

1. Na Interface do analista do Support Automation, clique na guia da ferramenta adequada para resolver o ticket:
   - Tarefas automatizadas: selecione uma tarefa automatizada na seção à esquerda e clique em Executar. Por exemplo, execute o script que configura as configurações de rede para o aplicativo de software.
   - Explorador de arquivos: procure o sistema de arquivos do usuário. Por exemplo, procure a unidade de disco rígido para localizar um arquivo específico no diretório de instalação do aplicativo do software.
   - Transferência de arquivo: transfira um arquivo entre computadores. Por exemplo, transfira um arquivo do seu computador para substituir um arquivo corrompido no diretório de instalação.
   - Registro remoto: procure o registro do usuário final e modifique a entrada do registro. Por exemplo, modifique os valores do registro do aplicativo de software.
   - Ferramentas remotas do sistema: execute um programa no computador do usuário final ou force a reinicialização do computador. Por exemplo, execute a interface de configuração do aplicativo do software.
   - Controle remoto: controle remotamente o computador do usuário final. Por exemplo, controle o computador do usuário final a fim de configurar o software aplicativo.
   - Captura de tela: faça uma captura da tela do computador do usuário final. Por exemplo, problemas de conexão impedem o controle remoto de operar com êxito para guiar o usuário depois de exibir a captura de tela.
2. Selecione Controle remoto e configure o aplicativo de software para sincronizar com a rede da empresa.
3. Verifique com o usuário se o software do aplicativo está bem sincronizado e se você resolveu o ticket.

Encerre a sessão de assistência e feche o ticket.

Depois de verificar que o ticket foi resolvido, atualize o ticket e feche a sessão de assistência.

Siga estas etapas:

1. Clique em Finalizar na Interface do analista do Support Automation para fechar a sessão.

   O usuário recebe uma notificação por email com o log da sessão.

2. (Opcional) Clique no Log da sessão para exibir logs e os resultados da ferramenta do Support Automation.

3. Clique no número do ticket na interface de analista do Support Automation. Por exemplo, clique no Incidente 40.

   A página Detalhes do incidente 40 é aberta no CA SDM.

4. Clique em Editar.

5. Altere o status do ticket para Automação de suporte – Resolvido.

6. Clique em Salvar e fechar.

   O log de atividade do ticket é salvo e o processo de Assistência online é concluído.

Apêndice A: Exibir descrições de campo

Esta seção contém os seguintes tópicos:

Exibir descrições de campo (na página 1084)
View_Act_Log (na página 1084)
View_Audit_Assignee (na página 1086)
View_Audit_Group (na página 1087)
View_Audit_Priority (na página 1087)
View_Audit_Status (na página 1088)
View_Change_Act_Log (na página 1089)
View_Change (na página 1090)
View_Change_to_Assets (na página 1096)
View_Change_to_Change_Act_Log (na página 1097)
View_Change_to_Change_WF (na página 1098)
View_Change_to_Properties (na página 1100)
View_Contact_Full (na página 1102)
View_Contact_to_Environment (na página 1105)
View_Group (na página 1106)
View_Group_to_Contact (na página 1107)
View_Issue (na página 1107)
View_Issue_Act_Log (na página 1113)
View_Issue_to_Assets (na página 1114)
View_Issue_to_Issue_Act_Log (na página 1115)
View_Change_to_Request (na página 1116)
View_Issue_to_Issue_WF (na página 1120)
View_Issue_to_Properties (na página 1123)
View_Request (na página 1124)
View_Request_to_Act_Log (na página 1129)
View_Request_to_Properties (na página 1130)

Exibir descrições de campo

Você pode usar as informações de descrição do campo nas exibições básicas e avançadas fornecidas com o CA SDM.

Os seguintes pontos se aplicam a muitas tabelas:

- Você deve ativar o log de auditoria, encontrado em Administração, Gerenciador de opções, Log de auditoria para ver os dados nas exibições avançadas.

  Observação: para obter mais informações sobre o log de auditoria, consulte a *Ajuda online*.

- pdmtime faz referência aos campos data/hora que estão no formato GMT (o número de segundos decorridos desde 1/1/1970).
- Os termos solicitação de mudança e requisição de mudança podem ser trocados.

Mais informações:

Gerando relatórios no CA SDM (na página 889)

View_Act_Log

A seguir, uma exibição básica da tabela request activity log. O tipo de atividade e o nome completo do analista também estão listados na exibição. A tabela request activity log (act_log) foi unida à tabela Activity Type (act_type) e à tabela Contato (ca_contact) para fornecer o tipo de atividade real de cada entrada de log de atividades e o analista que executou a atividade. Campos extraídos das uniões que podem ser úteis estão localizados no final desta lista.

Campo	Observações
id	act_log.id: o identificador exclusivo para esse registro na tabela act_log.
persid	act_log.persid: o identificador exclusivo para esse registro na tabela act_log, precedido pelo identificador de objeto (alg para act_log) e dois pontos.
call_req_id	act_log.call_req_id: cursor para chamar solicitar persid ao qual esta atividade pertence. act_log.call_req_id = call_req.persid.
last_mod_dt	act_log.last_mod_dt: data/hora da última modificação (pdmtime).

Campo	Observações
time_spent	act_log.time_spent: tempo gasto nesta atividade, armazenado como o número total de segundos. Por exemplo, 80 = 1 minuto, 20 segundos.
time_stamp	act_log.time_stamp: data/hora da atividade, que pode ser modificada pelo usuário (pdmtime).
system_time	act_log.system_time: data/hora da criação do registro (pdmtime).
analista	act_log.analyst: o cursor de uuid para a uuid de contato para obter o analista que executou a atividade. act_log.analyst = ca_contact.contact_uuid.
descrição	act_log.description: descrição de texto desta atividade, que pode ser modificada pelo usuário.
action_desc	act_log.action_desc: descrição de texto de ação automatizada, que não pode ser modificada pelo usuário.
tipo	act_log.type: o cursor de texto para um registro na tabela do tipo de atividade. Por exemplo, act_log.type = act_type.code.
knowledge_session	act_log.knowledge_session: um identificador para uma determinada sessão de um determinado usuário.
knowledge_tool	act_log.knowledge_tool: um indicador da ferramenta de conhecimento usada para a pesquisa, como NLS_FAQ ou EXPERT, etc.
interno	act_log.internal: sinalizador de número inteiro (1 ou 0) que indica se essa entrada de log é para todos verem ou apenas para uso interno.
activity_type	act_type.symActivity: tipo derivado de act_log.type = act_type.code.
analyst_lastname	View_Contact_Full.last_name: o sobrenome do analista, derivado de act_log_analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: o nome do analista.
analyst_middlename	View_Contact_Full.middle_name: o nome do meio do analista.

View_Audit_Assignee

A seguir, uma exibição avançada do log de auditoria no qual o destinatário é rastreado. Essa exibição mostra a duração de tempo entre as mudanças do destinatário para cada solicitação e requisição de mudança. As solicitações ou requisições de mudança são mudadas de um determinado destinatário para um destinatário nulo e, em seguida, de um destinatário nulo para um determinado destinatário não têm a duração do destinatário nulo listada nessa exibição. Essa exibição lista os seguintes campos tanto para solicitações como para requisições de mudança. Pode haver mais de uma entrada por audobj_uniqueid (solicitação ou requisição de mudança).

Campo	Observações
audobj_uniqueid	audit_log.audobj_uniqueid: a ID exclusiva do objeto de log de auditoria que representa chg.id ou call_req.id.
from_val	audit_log.attr_after_val: o valor de 'alterado de' do responsável
to_val	audit_log.attr_after_val: o valor de 'alterado para' do responsável.
from_time	audit_log.attr_from_time: o horário inicial no qual um responsável foi atribuído (pdmtime).
to_time	audit_log.attr_from_time: o horário final no qual o mesmo responsável foi atribuído (pdmtime).

View_Audit_Group

A seguir, uma exibição avançada do log de auditoria no qual o grupo é rastreado. Essa exibição mostra a duração de tempo entre as mudanças do grupo para cada solicitação e requisição de mudança. As solicitações ou requisições de mudança alteradas de um determinado grupo para um grupo nulo e, em seguida, de um nulo novamente para um determinado não têm a duração do grupo nulo listada nessa exibição. Essa exibição lista os seguintes campos tanto para solicitações como para requisições de mudança. Pode haver mais de uma entrada por audobj_uniqueid (solicitação ou requisição de mudança).

Campo	Observações
audobj_uniqueid	audit_log.audobj_uniqueid: a ID exclusiva do objeto de log de auditoria que representa chg.id ou call_req.id.
from_val	audit_log.attr_after_val: o valor de ‘alterado de’ do grupo.
to_val	audit_log.attr_after_val: o valor de ‘alterado para’ do grupo.
from_time	audit_log.attr_from_time: horário inicial no qual o grupo foi atribuído (pdmtime).
to_time	audit_log.attr_from_time: horário final no qual o mesmo grupo foi atribuído (pdmtime).

View_Audit_Priority

A seguir, uma exibição avançada do log de auditoria no qual a prioridade é rastreada. Essa exibição mostra a duração de tempo entre as mudanças da prioridade para cada solicitação e requisição de mudança. Essa exibição lista os seguintes campos tanto para solicitações como para requisições de mudança. Pode haver mais de uma entrada por audobj_uniqueid (solicitação ou requisição de mudança).

Campo	Observações
audobj_uniqueid	audit_log.audobj_uniqueid: a ID exclusiva do objeto de auditoria que representa uma solicitação call_req.id ou requisição de mudança chg.id.

Campo	Observações
from_val	audit_log.attr_after_val: o valor de prioridade de ‘alterado de’.
to_val	audit_log.attr_after_val: o valor de prioridade de ‘alterado para’.
from_time	audit_log.attr_from_time: o horário inicial no qual a prioridade estava em um determinado estado (pdmtime).
to_time	audit_log.attr_from_time: o horário final no qual a prioridade estava no mesmo estado (pdmtime).

View_Audit_Status

A seguir, uma exibição avançada do log de auditoria no qual o status é rastreado. Essa exibição mostra a duração de tempo entre as mudanças do status para cada solicitação e requisição de mudança. Essa exibição lista os seguintes campos tanto para solicitações como para requisições de mudança. Pode haver mais de uma entrada por audobj_uniqueid (solicitação ou requisição de mudança).

Campo	Observações
audobj_uniqueid	audit_log.audobj_uniqueid: a ID exclusiva do objeto de auditoria que representa uma solicitação call_req.id ou requisição de mudança chg.id.
from_val	audit_log.attr_after_val: o valor de prioridade de ‘alterado de’
to_val	audit_log.attr_after_val: o valor de prioridade de ‘alterado para’.
from_time	audit_log.attr_after_time: o horário inicial no qual o status estava em um determinado estado (pdmtime).
to_time	audit_log.attr_after_time: o horário final no qual o status estava no mesmo estado (pdmtime).

View_Change_Act_Log

A seguir, uma exibição básica de todos os logs de atividades de requisição de mudança. Essa é uma exibição da tabelacChange request activity log (chgalg) unida com a tabela activity type (act_type) e a tabela Contato (ca_contact) para fornecer dados mais significativos, como a descrição do tipo de atividade real e o nome completo do analista que executou a atividade.

Campo	Observações
id	chgalg.id: o identificador exclusivo para este registro na tabela chgalg.
persid	chgalg.persid: o identificador exclusivo para este registro na tabela chgalg, precedido pelo identificador de objeto (chgalg para chgalg) e dois pontos.
change_id	chgalg.change_id: o cursor para a id da requisição de mudança à qual esta atividade pertence. chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt: a última data/horário de modificação (pdmtime).
time_spent	chgalg.time_spent: a duração do tempo gasto nesta atividade, armazenada como o número total de segundos. Por exemplo, 80 = 1 minuto, 20 segundos.
time_stamp	chgalg.time_stamp: a data/horário, que pode ser modificada pelo usuário, da atividade (pdmtime).
system_time	chgalg.system_time: a data/horário da criação do registro (pdmtime).
analista	chgalg.analyst: o cursor uuid para a uuid de contato para obter o analista que executou a atividade. chgalg.analyst = ca_contact.contact_uuid
descrição	chgalg.description: a descrição do texto desta atividade, que pode ser modificada pelo usuário.
action_desc	chgalg.action_desc: a descrição de texto da ação automatizada, que não pode ser modificada pelo usuário.
tipo	chgalg.type: o cursor de texto para um registro na tabela de tipo de atividade. chgalg.type = act_type.code

Campo	Observações
interno	chgalg.internal: o sinalizador de número inteiro (1 ou 0), que indica se a entrada do log deve ser vista por todos ou se é apenas para uso interno.
knowledge_session	chgalg.knowledge_session: um identificador para uma determinada sessão de um determinado usuário.
knowledge_tool	chgalg.knowledge_tool: um indicador da ferramenta de conhecimento usado para pesquisa, tal como NLS_FAQ ou EXPERT, etc.
analyst_lastname	View_Contact_Full.last_name: o sobrenome do analista, derivado de chgalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: o nome do analista.
analyst_middlename	View_Contact_Full.middle_name: o nome do meio do analista.
activity_type	act_type.sym: tipo de atividade mencionado por chgalg.type = act_type.code.

View_Change

A seguir, uma exibição básica de todas as requisições de mudança, listando o status, a prioridade, a categoria, as organizações, o nome completo do usuário final afetado, o nome completo do solicitante, o nome completo do destinatário, o nome do grupo e ID e assim por diante. Aqui, a tabela change request (chg) foi unida a muitas outras tabelas para fornecer dados mais significativos sobre a requisição de mudança.

Campo	Observações
id	chg.id: o identificador exclusivo para esse registro na tabela chg.
persid	chg.persid: um identificador exclusivo para esse registro na tabela chg, precedido pelo identificador de objeto (chg para tabela chg) e dois pontos.
chg_ref_num	chg.chg_ref_num: o número de referência da requisição de mudança usado pelos analistas e clientes para fazer referência a uma determinada requisição de mudança.

Campo	Observações
descrição	chg.description: a descrição longa de requisição de mudança, como estabelecido por um analista ou cliente.
status	chg.status: o identificador exclusivo de um status de requisições de mudança, que é um cursor para a tabela chgstat. chg.status = chgstat.code.
active_flag	chg.active_flag: sinalizador de número inteiro para determinar se esse registro de mudança está ativo ou não (1 ou 0).
start_date	chg.start_date: a data em que a primeira tarefa vai para um status pendente (pdmtime).
open_date	chg.open_date: a data da criação da requisição de mudança (pdmtime)
last_mod_dt	chg.last_mod_dt: A data da última modificação (pdmtime).
last_mod_by	chg.last_mod_by: O cursor para a uuid de contato que foi o último contato a modificar essa requisição de mudança. chg.last_mod_by = ca_contact.contact_uuid.
close_date	chg.close_date: a data em que a requisição de mudança foi definida como inativo (pdmtime).
resolve_date	chg.resolve_date: a data na qual a requisição de mudança foi definida para um status configurado para indicar que a mudança foi resolvida (pdmtime).
rootcause	chg.rootcause: Um cursor para um registro na tabela rootcause, que representa a situação original que exigiu que essa requisição de mudança fosse executada. chg.rootcause = rootcause.id.
est_total_time	chg.est_total_time: O tempo total estimado (pdmtime) que levará para concluir essa mudança.
actual_total_time	chg.actual_total_time: O tempo total real (pdmtime) gasto para concluir essa mudança.
log_agent	chg.log_agent: Um identificador exclusivo binário que se refere à tabela ca_contact, fazendo menção à pessoa que foi o criador original da mudança. chg.log_agent = ca_contact.contact_uuid.
responsável	chg.assignee: O cursor para a uuid de contato que está atualmente atribuído à requisição de mudança. chg.assignee = ca_contact.contact_uuid.

Campo	Observações
empresa	chg.organization: O cursor para a uuid interna de organização, que representa a empresa a quem esta requisição de mudança pertence. chg.organization = ca_organization.organization_uuid.
group_id	chg.group_id: O cursor para a uuid de contato, que representa o grupo atualmente atribuído à requisição de mudança. chg.group_id = ca_contact.contact_uuid
affected_contact	chg.affected_contact: O cursor para a uuid de contato, que representa o contato afetado para essa requisição de mudança. chg.affected_contact = ca_contact.contact_uuid
requestor	chg.requrestor: O cursor para a uuid de contato, que representa a pessoa que solicitou a mudança. chg.requestor = ca_contact.contact_uuid
categoria	chg.category: O cursor para o código de categoria de mudança para obter a categoria na qual essa mudança se encaixa. chg.category = chgcat.code
priority	chg.priority: O cursor para a prioridade enum, que representa a prioridade na qual essa mudança se encaixa. chg.priority = pri.enum
need_by	chg.need_by: A data que indica quando affected_end_user precisa que a mudança esteja concluída (pdmtime).
est_comp_date	chg.est_comp_date: A data estimada da conclusão (pdmtime) desta Requisição de mudança.
actual_comp_date	chg.actual_comp_date: Data real da conclusão (pdmtime) desta requisição de mudança.
est_cost	chg.est_cost: O custo estimado desta requisição de mudança.
actual_cost	chg.actual_cost: O custo real para implementar essa requisição de mudança.
justificativa	chg.justification: Um campo de texto que permite que um solicitante documente os motivos pelos quais essa mudança é necessária.
backout_plan	chg.backout_plan: Um campo de texto que permite que um analista documente um plano de retrocesso para essa mudança.

Campo	Observações
impact	chg.impact: Um cursor para um registro de tabela impact, que indica o escopo dos recursos que essa mudança afeta. chg.impact = impact.enum
pai	chg.parent: Um cursor para outra ID de requisição de mudança, que permite a criação de uma hierarquia de requisições de mudança. chg.parent = chg.id
effort	chg.esforço: Um campo de texto que explica o plano para implementação desta requisição de mudança.
support_lev	chg.support_lev: Um cursor para um registro desc de serviço, que automatiza algumas restrições para a qual essa mudança deve ser concluída. chg.support_lev = srv_desc.code
template_name	chg.template_name: Um nome e um cursor para um modelo de requisição de mudança. chg.template_name = chg_template.template_name
sla_violation	chg.sla_violation: O número inteiro para contar o número de vezes que os SLAs anexados a essa "mudança foram violados".
predicted_sla_viol	chg.predicted_sla_viol: (r5.5) Campo de tecnologia relacionado ao Neugent.
macro_predict_viol	chg.macro_predicted_viol: (r5.5) Campo de tecnologia relacionado ao Neugent.
created_via	chg.created_via: Um cursor para um registro na tabela interface, que indica de qual interface a requisição de mudança foi originada. chg.created_via = interface.id
call_back_date	chg.call_back_date: Um campo de data/hora (pdmtime) que indica uma data/hora no futuro na qual o solicitante deverá ser contatado.
call_back_flag	chg.call_back_flag: Um indicador booleano exibido como caixa de seleção ao usuário, indicando se deve ou não notificar o analista na chg.call_back_date.
sequência de caracteres1	É um campo de texto definido pelo usuário.
sequência de caracteres2	É um campo de texto definido pelo usuário.
sequência de caracteres3	É um campo de texto definido pelo usuário.
sequência de caracteres4	É um campo de texto definido pelo usuário.

Campo	Observações
sequência de caracteres5	É um campo de texto definido pelo usuário.
sequência de caracteres6	É um campo de texto definido pelo usuário.
service_date	chg.service_date: a Data/Hora (pdmtime) que se espera que um fornecedor externo gaste para atender a essa requisição de mudança.
service_num	chg.service_num: campo de texto para documentar um serviço de fornecedor externo ou número do pedido de compra.
product	chg.product: um cursor para um registro na tabela product, que indica o produto afetado por essa mudança. chg.product = product.id
ações	chg.actions: campo de texto grande para documentação das ações.
type_of_contact	chg.type_of_contact: um cursor para um registro na tabela toc, que indica uma categorização geral da perspectiva da requisição de mudança do affected_end_user. chg.type_of_contact = toc.id
reporting_method	chg.reporting_method: um cursor para um registro na tabela repmeth, que classifica a origem da requisição de mudança e é selecionado pela pessoa que está criando a requisição de mudança. chg.reporting_method = repmeth.id
person_contacting	chg.person_contacting: um cursor para um registro na tabela perscon, que indica a função do affected_end_user ou solicitante. chg.person_contacting = perscon.id
status_name	chgstat.sym: a descrição do status como visto por um usuário. chg.status = chgstat.code
priority_num	pri.sym: a descrição da prioridade como vista por um usuário. chg.priority = pri.enum
category_name	chgcat.sym: o nome da Categoria de mudança como visto por um usuário. chg.category = chgcat.code
organization_name	ca_organization.org_name: o nome de uma organização como vista por um usuário. chg.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: o sobrenome do usuário final afetado. chg.affected_end_user = ca_contact.contact_uuid

Campo	Observações
affected_end_user_firstname	ca_contact.first_name: o nome do usuário final afetado. chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: o nome do meio do usuário final afetado. chg.affected_end_user = ca_contact.contact_uuid
requester_lastname	ca_contact.last_name: o sobrenome do solicitante. chg.requestor = ca_contact.contact_uuid
requester_firstname	ca_contact.first_name: o nome do solicitante. chg.requestor = ca_contact.contact_uuid
requester_middlename	ca_contact.middle_name: o nome do meio do solicitante. chg.requestor = ca_contact.contact_uuid
comercial	ca_organization.org_name: o nome da organização do Solicitante como visto pelos usuários. chg.requestor = ca_organization.organization_uuid
assignee_lastname	ca_contact.last_name: o sobrenome do responsável. chg.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: o nome do responsável. chg.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: o nome do meio do responsável. chg.assignee = ca_contact.contact_uuid
groupID	ca_contact.contact_uuid: uma representação binária da id interna usada para o grupo atribuído a essa requisição de mudança. chg.group_id = ca_contact.contact_uuid
group_name	ca_contact.last_name: o nome do grupo atribuído a essa requisição de mudança. chg.group = ca_contact.contact_uuid
service_type	srv_desc.sym: o nome do tipo de serviço aplicado a essa requisição de mudança. chg.support_lev = srv_desc.code
impact_num	impact.sym: a descrição do impacto como vista pelos usuários. chg.impact = impact.enum
product_sym	product.sym: a descrição do produto como vista pelos usuários. chg.product = product.id
type_of_contact_sym	toc.sym: A descrição do Tipo de contato como vista pelos usuários. chg.type_of_contact = toc.id

Campo	Observações
rpting_method_sym	repmeth.sym: a descrição do Método de relatar conforme vista pelos usuários. chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: a descrição do Contato responsável conforme vista pelos usuários. chg.person_contacting = perscon.id

View_Change_to_Assets

A lista de campos a seguir é uma exibição básica das requisições de mudança e seus ativos. A tabela change request (chg) está unida indiretamente à tabela network resource (ca_owned_resource) para obter uma lista de ativos de cada requisição de mudança. Essa exibição talvez não liste todas as requisições de mudança, especialmente aquelas que não possuem ativos.

Campo	Observações
View_Change.*	Todos os campos listados na exibição View_Change definida anteriormente neste documento.
assetID	ca_owned_resource.own_resource_uuid: o campo binário que serve como o identificador exclusivo inalterável e interno de um registro de ativo.
asset_serial_num	ca_owned_resource.serial_number: o número de série de um registro de ativo.
asset_class	ca_resource_class.name: uma descrição breve da classe à qual um ativo pertence. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: a família de ativos à qual o ativo pertence. ca_owned_resource.resource_class = ca_resource_class.id E ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name: o nome de rede pelo qual o ativo é conhecido.

View_Change_to_Change_Act_Log

A seguir, uma exibição básica de todas as requisições de mudança e os logs de atividades que as acompanham. Essa exibição se une à exibição View_Change com o Log de atividades de requisição de mudança (chgalg) para dar informações detalhadas sobre as requisições de mudança e seus logs de atividades.

Campo	Observações
View_Change.*	Mostra todos os campos listados na exibição View_Change definida anteriormente neste documento.
chgalg_id	chgalg.id: o identificador exclusivo para este registro na tabela chgalg.
chgalg_persid	chgalg.persid: o identificador exclusivo para este registro na tabela chgalg, precedido pelo identificador de objeto (chgalg para chgalg) e dois pontos.
change_id	chgalg.change_id: um cursor para alterar a ID da requisição à qual essa atividade pertence. chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt: a última data/horário de modificação (pdmtime).
time_spent	chgalg.time_spent: a duração do tempo gasto nesta atividade, armazenada como o número total de segundos. Por exemplo, 80 = 1 minuto, 20 segundos.
time_stamp	chgalg.time_stamp: a data/horário, que pode ser modificada pelo usuário, da atividade (pdmtime).
system_time	chgalg.system_time: a data/horário da criação do registro (pdmtime).
analista	chgalg.analyst: o cursor uuid para a uuid de contato para obter o analista que executou a atividade. chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description: a descrição do texto desta atividade, que pode ser modificada pelo usuário.
action_desc	chgalg.action_desc: descrição de texto da ação automatizada, que não pode ser modificada pelo usuário.

Campo	Observações
tipo	chgalg.type: o cursor de texto para um registro na tabela de tipo de atividade. chgalg.type = act_type.code
interno	chgalg.internal: o sinalizador de número inteiro (1 ou 0), que indica se a entrada do log deve ser vista por todos ou se é apenas para uso interno.
knowledge_session	chgalg.knowledge_session: um identificador para uma determinada sessão de um determinado usuário.
knowledge_tool	chgalg.knowledge_tool: um indicador da ferramenta de conhecimento usado para a pesquisa, tal como NLS_FAQ ou EXPERT, etc.
chgalg_analyst_id	chgalg.analyst: este é o cursor de uuid para a uuid de contato para obter o analista que executou a atividade. chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

Essa exibição é um resultado da exibição View_Change unida à tabela de tarefa Workflow (wf) para oferecer uma exibição básica da requisição de mudança e suas tarefas de fluxo de trabalho. Talvez isso não liste todas as requisições de mudança, particularmente quando não há tarefas de fluxo de trabalho atribuídas.

Campo	Observações
View_Change.*	Mostra todos os campos listados na exibição View_Change definida anteriormente neste documento.
wf_id	wf.id: o identificador exclusivo para um registro na tabela wf.
wf_persid	wf.persid: um identificador exclusivo para esse registro na tabela wf, precedido pelo identificador de objeto (wf para wf) e dois pontos.
del	wf.del: um indicador booleano. Especifica se esse registro deve ser exibido ao usuário.
object_type	wf.object_type: o nome de fábrica usado para identificar o tipo de registro (por exemplo, chg) para o qual essa tarefa de fluxo de trabalho está anexada.

Campo	Observações
object_id	wf.object_id: o identificador exclusivo usado para identificar o registro específico ao qual essa tarefa de fluxo de trabalho está anexada. wf.object_id = chg.id
tarefa	wf.task: um identificador que se refere ao tipo de tarefa que esse registro representa. wf.task = tskty.code
wf_template	wf.wf_template: um identificador que faz referência a partir de qual modelo esse registro de tarefa de fluxo de trabalho foi criado. wf.wf_template = wftpl.id
seqüência	wf.sequence: este é um número inteiro que indica a ordem na qual esse determinado registro de tarefa de fluxo de trabalho deve ser exibido e executado pelo CA SDM (por exemplo, Ascendente).
wf_status	wf.status: este é um identificador que faz referência a um registro tskstat que indica o status atual desta tarefa de fluxo de trabalho. wf.status = tskstat.code
group_task	wf.group_task: um Booleano, que indica se essa tarefa pertence a um grupo.
ativo	wf.asset: este é um identificador da UUID (binária) que faz referência a um registro na tabela ca_owned_resource. wf.asset = ca_owned_resource.own_resource_uuid
criador	wf.creator: um identificador da UUID (binária) que faz referência a um registro na tabela ca_contact. Indica a pessoa que criou essa tarefa de fluxo de trabalho. wf.creator = ca_contact.contact_uuid
date_created	wf.date_created: a Data/Carimbo de data e hora na qual essa tarefa de fluxo de trabalho foi criada (pdmtime).
wf_assignee	wf.assignee: o identificador da UUID (binária) que faz referência a um registro na tabela ca_contact. Indica a pessoa que está atribuída atualmente a essa tarefa de fluxo de trabalho. wf.assignee = ca_contact.contact_uuid
done_by	wf.done_by: identificador da UUID (binária) que faz referência a um registro na tabela ca_contact. Indica a pessoa que concluiu ou aprovou essa tarefa de fluxo de trabalho. wf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: o carimbo de data/hora em que a tarefa de fluxo de trabalho passou para um status ativo (pdmtime).

Campo	Observações
wf_est_comp_date	wf.est_comp_date: o carimbo de data/hora (pdmtime) que os usuários acreditam que essa tarefa será concluída.
est_duration	wf.est_duration: a duração estimada para essa tarefa de fluxo de trabalho.
completion_date	wf.completion_dat: o carimbo de data/hora (pdmtime) em que essa tarefa de fluxo de trabalho foi concluída.
actual_duration	wf.actual_duration: a quantia real de tempo que levou para concluir essa tarefa de fluxo de trabalho.
wf_est_cost	wf.est_cost: o custo estimado para essa tarefa de fluxo de trabalho.
custo	wf.cost: o custo real exigido para concluir essa tarefa de fluxo de trabalho.
wf_description	wf.description: a descrição da tarefa de fluxo de trabalho.
wf_last_mod_dt	wf.last_mod_dt: o carimbo de data/hora (pdmtime) em que essa tarefa de fluxo de trabalho foi alterada pela última vez.
wf_last_mod_by	wf.last_mod_by: o identificador exclusivo da UUID (binária) que faz referência a um registro na tabela contact, que indica a última pessoa a fazer mudanças a essa tarefa de fluxo de trabalho. wf.last_mod_by = ca_contact.contact_uuid

View_Change_to_Properties

Essa exibição é um resultado da exibição View_Change unida com a tabela Properties (prp) para fornecer uma exibição básica da requisição de mudança e suas propriedades atribuídas. Talvez isso não liste todas as requisições de mudança, particularmente quando não há propriedades atribuídas.

Campo	Observações
View_Change.*	Mostra todos os campos listados na exibição View_Change definida anteriormente neste documento.
prp_id	prp.id: um identificador de número inteiro exclusivo para o registro de propriedade.
prp_persid	prp.persid: um identificador exclusivo para esse registro na tabela wf, precedido pelo identificador de objeto (prp para prp) e dois pontos.

Campo	Observações
object_type	prp.object_type: o nome de fábrica usado para identificar o tipo de registro (por exemplo, chg) para o qual esse registro de propriedade está anexado.
object_id	prp.object_id: o identificador exclusivo usado para identificar o registro específico ao qual essa propriedade está anexada. prp.object_id = chg.id
seqüência	prp.sequence: um número inteiro que indica a ordem na qual esse registro de propriedade particular deve ser exibido pelo CA SDM (por exemplo, Ascendente.)
propriedade	prp.property: um identificador que faz referência a um registro na tabela prptpl. Representa o modelo a partir do qual essa propriedade foi criada. prp.property=prptpl.code
valor	prp.value: o valor inserido pelo usuário em resposta aos campos prp_description e prp.label.
prp_last_mod_dt	prp.last_mod_dt: o carimbo de data/hora (pdmtime) de quando essa propriedade foi modificada pela última vez.
prp_last_mod_by	prp.last_mod_by: um identificador binário que faz referência a um registro na tabela ca_contact. Representa a pessoa que fez a última modificação nesse registro. prp.last_mod_by = ca_contact.contact_uuid
obrigatório	prp.required: um Booleano indicando se essa propriedade deve ter um prp.value antes de o registro ser salvo.
exemplo	prp.sample: um campo de texto que exibe valores de exemplo para guiar o usuário, digitando o valor mais útil em prp.value.
prp_description	prp.description: um campo de texto que explica que tipo de valor deve ser inserido em prp.value.
rótulo	prp.label: uma descrição curta sobre o que deve ser colocado no campo prp.value.

View_Contact_Full

Os campos a seguir são uma exibição básica de todos os contatos. Essa exibição lista todos os campos na tabela ca_contact, mais os campos de referência como as descrições curtas para tipo de contato, nome de local, nomes da organização e tipo de serviço de cada contato. Essa exibição já foi ligada às tabelas ca_location, ca_organization, srv_desc e ca_contact_type para obter os nomes e símbolos reais para alguns campos na tabela ca_contact. Os nomes e símbolos reais estão localizados no final dessa lista de campos da exibição.

Campo	Observação
contact_uuid	ca_contact.contact_uuid: um identificador binário exclusivo para cada registro ca_contact.
middle_name	ca_contact. middle_name: o nome do meio deste contato.
alias	ca_contact.alias: o nome alternativo, frequentemente informal deste contato
last_name	ca_contact.last_name: o sobrenome do contato.
first_name	ca_contact.first_name: o nome formal do contato
pri_phone_number	ca_contact.pri_phone_number: o número de telefone principal do contato.
alt_phone_number	ca_contact.alt_phone_number:o número de telefone alternativo do contato
fax_number	ca_contact.fax_number: o número de fax do contato.
mobile_phone	ca_contact.mobile_phone: número do telefone celular do contato.
pager_number	ca_contact.pager_number: o número para emitir uma página para a página do contato.
email_address	ca_contact.email_address: o endereço de email do contato.
location_uuid	ca_contact.location_uuid: um identificador binário exclusivo que faz referência a um registro na tabela ca_location, que indica o local estático do contato. ca_contact.location_uuid = ca_location.location_uuid
floor_location	ca_contact.floor_location: o número do andar do contato.
pager_email_address	ca_contact.pager_email_address: um endereço de email do pager do contato.

Campo	Observação
room_location	ca_contact.room_location: a sala específica do contato no andar no local estático.
contact_type	ca_contact.contact_type: um identificador de número inteiro exclusivo, que faz referência a uma linha na tabela ca_contact_type, que indica a função geral desse contato dentro do aplicativo Service Desk. ca_contact.contact_type = ca_contact_type.id
inactive	ca_contact.inactive: um indicador booleano do estado deste registro, determinando sua inclusão ou exclusão a partir de pesquisas padrão no Service Desk.
creation_user	ca_contact.creation_user: a id de usuário do contato que criou esse registro. ca_contact.creation_user = ca_contact.userid
creation_date	ca_contact.creation_date: um carimbo de data/hora (pdmtime) que indica a data e hora em que esse contato foi criado.
last_update_user	ca_contact.last_update_user: uma id de usuário do contato que atualizou o registro de contato pela última vez. ca_contact.last_update_user = ca_contact.userid
last_update_date	ca_contact.last_update_date: um carimbo de data/hora (pdmtime) que indica a data e a hora da última modificação deste registro.
version_number	ca_contact.version number: o indicador interno de versão.
departamento	ca_contact.department: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela ca_resource_department, que indica o departamento do contato. ca_contact.department = ca_resource_department.id
comment	ca_contact.comment: um campo de comentário de texto livre para os analistas documentarem fatos importantes que influenciam o tratamento desse contato em particular.
company_uuid	ca_contact.company_uuid: um identificador binário exclusivo que faz referência a uma linha na tabela ca_company. Indica a afiliação desse contato com uma empresa. ca_contact.company_uuid = ca_company.company_uuid

Campo	Observação
organization_uuid	ca_contact.organizaiton_uuid: um identificador binário exclusivo que faz referência a uma linha na tabela ca_organization. Indica a organização na qual esse contato trabalha. ca_contact.organizaiton_uuid = ca_organization.organization_uuid
admin_organization_uuid	ca_contact.admin_organization_uuid: um identificador binário exclusivo que faz referência a uma linha na tabela ca_organization. Indica a organização administrativa desse contato. ca_contact.admin_organization_uuid = ca_organization.organization_uuid
alternate_identifier	ca_contact.alternate_identifier: um identificador definido pelo usuário, normalmente uma entidade usada pelo recursos humanos exclusivamente para identificar esse contato.
job_title	ca_contact.job_title: um identificador exclusivo de número inteiro que faz referência à tabela ca_job_title. Indica o título da tarefa padronizado para esse contato. ca_contact.job_title = ca_job_title.id
job_function	ca_contact.job_function: um identificador exclusivo de número inteiro que faz referência à tabela ca_job_function. Indica uma descrição geral padronizada da função da tarefa do contato. ca_contact.job_function = ca_job_function.id
mail_stop	ca_contact.mail_stop: interrupção de correio
cost_center	ca_contact.cost_center: um identificador exclusivo de número inteiro que faz referência à tabela ca_resource_cost_center. Indica o centro de custos principal desse contato. ca_contact.cost_center = ca_cost_center.id
id do usuário	ca_contact.userid: o identificador de usuário que esse contato usará para efetuar o logon no Service Desk.
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid: um identificador binário exclusivo que faz referência a uma linha na tabela ca_contact, que cria uma hierarquia de contatos para indicar a estrutura de relatório de cada contato. ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid
exclude_registration	ca_contact.exclude registration: um sinalizador interno.
delete_time	ca_contact.delete_time: um carimbo de data/hora que indica quando o sinalizador inativo foi definido como 1.

Campo	Observação
contact_type_name	ca_contact_type.name: uma descrição curta do ca_contact.contact_type desse contato.
location_name	ca_location.name: uma descrição curta do local estático desse contato.
organização	ca_organization.org_name: uma descrição curta do ca_contact.organizaiton_uuid desse contato
admin_organization	ca_organization.org_name: uma descrição curta do nome da organização desse contato. ca_contact.admin_organization_uuid
service_type	srv_desc.sym: uma descrição curta do usp_contact.c_service_type desse contato. ca_contact.contact_uuid = usp_contact.contact_uuid E usp_contact.c_service_type = srv_desc.code
state_sym	ca_location.state: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela ca_state_provice que indica o Estado, Província ou outra região geográfica artificialmente definida. ca_contact.location_uuid = ca_location.location_uuid E ca_location.state = ca_state_province.id

View_Contact_to_Environment

A lista de campos a seguir é uma exibição básica dos contatos e seus ambientes (ativos). Essa exibição é uma exibição da tabela Contato (ca_contact), mas também está ligada à tabela Owned Resource (ca_owned_resource) para obter uma lista de todos os ativos associados a um contato. Essa exibição pode ser estar ligada à exibição View_Contact_Full para obter o tipo de contato, tipo de serviço, organizações e local de cada contato. Ou essa exibição pode estar ligada às tabelas individuais para obter as mesmas informações.

Campo	Observações
ca_contact.*	Os campos ca_contact que estão definidos na definição de exibição View_Contact_Full.
asset_uuid	ca_owned_resource.own_resource_uuid: um identificador binário exclusivo para um ativo na tabela ca_owned_resource.

Campo	Observações
asset_name	ca_owned_resource.resource_name: o nome designado de rede deste ativo.

View_Group

A lista de campos a seguir é uma exibição básica da tabela de contatos, mas lista apenas os contatos do grupo. ID de tipo de contato = 2308, que é para tipos de grupo. Talvez você queria ligar essa exibição a outras tabelas do CA SDM para obter dados mais significativos para a emissão de relatórios. Por exemplo, é possível uni-la à tabela Location (ca_location) para encontrar o nome e endereço para o local do local do grupo. Também é possível unir essa exibição à tabela Organization (ca_organization) para obter os nomes da organização administrativa e funcional para o grupo.

Campo	Observações
ca_contact.*	Os campos ca_contact que estão definidos na definição de exibição View_Contact_Full.

O exemplo a seguir mostra como funciona a união de tabelas e como os campos relatar são extraídos. O campo de uma tabela (à direita) é unido (->) a um campo de outra tabela (à esquerda). Para fazer a união adequada entre tabelas e exibições, você precisa entender as diferenças nas uniões para o banco de dados. O campo definido nos parênteses, como pode ser visto a seguir, é o que você pode querer usar em seus relatórios se as tabelas anteriores forem unidas na exibição View_Group:

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid (ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid (ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid (ca_organization(2). org_name)

View_Group_to_Contact

A lista de campos a seguir é uma exibição básica de todos os contatos de grupo (membros). Também inclui os gerentes. Aqui, View_Group está unida à tabela Group_Member e, em seguida, unido à tabela ca_contact. Todos os campos em View_Group estão listados, bem como o nome, nome do meio e sobrenome da tabela ca_contact. O sinalizador de gerente Group_Member também está listado. O sinalizador de gerente de membro do grupo é 1 ou 0, o que significa que o membro é um gerente (sim - 1) ou não é um gerente (não - 0). A maioria das informações dessa exibição pertence ao grupo em si, não aos membros reais. Essa exibição é usada para localizar informações em um determinado grupo, incluindo os nomes de seus membros.

Campo	Observações
View_Group.*	Os campos View_Group que são especificados na definição View_Group.
member_lastname	ca_contact.last_name: o sobrenome do membro do grupo.
member_firstname	ca_contact.first_name: o nome formal do membro do grupo.
member_middlename	ca_contact.middle_name: o nome do meio do membro do grupo.
grpmem_manager_flag	ca_contact.manager_flag: o indicador de Gerente de membro do grupo (1 ou 0).

View_Issue

A seguir, uma exibição básica de todas as ocorrências, listando o status, a prioridade, a categoria, as organizações, o nome completo do solicitante, o nome completo do destinatário, o nome do grupo e ID e assim por diante. Aqui, a tabela issue está unida a muitas outras tabelas para fornecer alguns dados mais significativos sobre a ocorrência.

Campo	Observações
id	issue.id: O identificador exclusivo para esse registro na tabela issue.
persid	issue.persid: O identificador exclusivo para esse registro na tabela issue, precedido pelo identificador de objeto (iss para a tabela de ocorrência) e dois pontos.

Campo	Observações
issue_ref_num	issue.iss_ref_num: Número de referência da ocorrência usado pelos analistas e clientes para fazer referência a uma determinada ocorrência.
descrição	issue.description: A descrição longa de uma ocorrência como estabelecido por um analista ou cliente.
status	issue.status: O identificador exclusivo de um status de ocorrência, que é um cursor para a tabela issstat: issue.status = issstat.code
active_flag	issue.active_flag: O sinalizador de número inteiro para determinar se essa ocorrência está ativa (1 ou 0).
start_date	issue.start_date: A data em que a primeira tarefa vai para um status pendente (pdmtime).
open_date	issue.open_date: A data da criação da ocorrência (pdmtime)
last_mod_dt	issue.last_mod_dt: A data da última modificação (pdmtime)
last_mod_by	issue.last_mod_by: O ponteiro para a uuid de contato que foi o último contato a modificar essa ocorrência. issue.last_mod_by = ca_contact.contact_uuid
close_date	issue.close_date: A data em que a ocorrência foi definida como inativa (pdmtime).
resolve_date	issue.resolve_date: A data na qual a ocorrência foi definida para um status configurado para indicar que a ocorrência foi resolvida (pdmtime).
rootcause	issue.rootcause: Um cursor para um registro na tabela rootcause, que representa a situação original que exigiu que essa ocorrência fosse executada. issue.rootcause = rootcause.id
est_total_time	issue.est_total_time: Tempo total estimado (pdmtime) que levará para concluir essa ocorrência.
actual_total_time	issue.actual_total_time: Tempo total real (pdmtime) que levou para concluir essa ocorrência.
log_agent	issue.log_agent: Um identificador exclusivo binário que faz referência à tabela ca_contact, que, por sua vez, faz referências à pessoa que criou a ocorrência originalmente. issue.log_agent = ca_contact.contact_uuid

Campo	Observações
responsável	issue.assignee: O ponteiro para a uuid de contato que está atualmente atribuída à requisição de mudança. issue.assignee = ca_contact.contact_uuid
organização	issue.organization: O ponteiro para a uuid interna de organização, que representa a organização à qual esta ocorrência pertence. issue.organization = ca_organization.organization_uuid
group_id	issue.group_id: O ponteiro para a uuid de contato, que representa o grupo atualmente atribuído à ocorrência. issue.group_id = ca_contact.contact_uuid
affected_contact	issue.affected_contact: Um ponteiro para a uuid de contato, que representa o contato afetado por essa ocorrência. issue.affected_contact = ca_contact.contact_uuid
requestor	issue.requrestor: Um ponteiro para a uuid de contato, que representa a pessoa que pediu que essa ocorrência fosse registrada. issue.requestor = ca_contact.contact_uuid
categoria	issue.category: um cursor para o código de categoria de ocorrência para fazer referência à categoria na qual essa ocorrência se encaixa. issue.category = isscat.code
priority	issue.priority: um cursor para a prioridade enum, que representa a prioridade na qual essa ocorrência se encaixa. issue.priority = pri.enum
need_by	issue.need_by: Data que indica quando affected_end_user precisa que a ocorrência esteja concluída (pdmtime)
est_comp_date	issue.est_comp_date: Data estimada para a conclusão (pdmtime) desta ocorrência.
actual_comp_date	issue.actual_comp_date: Data real de conclusão (pdmtime) desta ocorrência.
est_cost	issue.est_cost: Custo estimado desta ocorrência.
actual_cost	issue.actual_cost: Custo real para implementar essa ocorrência.
justificativa	issue.justification: Um campo de texto que permite que um solicitante documente os motivos pelos quais essa ocorrência é necessária.
backout_plan	issue.backout_plan: Um campo de texto que permite que um analista documente um plano de retrocesso para essa ocorrência.

Campo	Observações
impact	issue.impact: um cursor para um registro de tabela impact, que indica o escopo dos recursos que essa ocorrência afeta. issue.impact = impact.enum
pai	issue.parent: um cursor para outra ID de ocorrência, que permite a criação de uma hierarquia de ocorrências. issue.parent = issue.id
effort	issue.effort: Um campo de texto que explica o plano para implementação desta ocorrência.
support_lev	issue.support_lev: um cursor para um registro desc de serviço, que automatiza algumas restrições sob as quais essa ocorrência deve ser concluída. issue.support_lev = srv_desc.code
template_name	issue.template: O nome de um modelo de ocorrência e o cursor para ele. issue.template_name = iss_template.template_name
sla_violation	issue.sla_violation: O número inteiro para contar o número de vezes que os SLAs vinculados a essa ocorrência foram violados.
predicted_sla_viol	issue.predicted_sla_viol: (r5.5) Campo de tecnologia relacionado ao Neugent.
macro_predict_viol	issue.macro_predict_viol: (r5.5) Campo de tecnologia relacionado ao Neugent
created_via	issue.created_via: um cursor para um registro na tabela interface. Isso indica a partir de qual interface a ocorrência foi originada. issue.created_via = interface.id
call_back_date	issue.call_back_date: Um campo de data e hora (pdmtime) que indica uma data/hora no futuro na qual o solicitante deverá ser contatado.
call_back_flag	issue.call_back_flag: Um indicador booleano exibido como uma caixa de seleção ao usuário, para indicar se o analista deve ser notificado ou não na issue.call_back_date.
seqüência de caracteres1	É um campo de texto definido pelo usuário.
seqüência de caracteres2	É um campo de texto definido pelo usuário.
seqüência de caracteres3	É um campo de texto definido pelo usuário.
seqüência de caracteres4	É um campo de texto definido pelo usuário.
seqüência de caracteres5	É um campo de texto definido pelo usuário.

Campo	Observações
seqüência de caracteres6	É um campo de texto definido pelo usuário.
service_date	issue.service_date: A Data/Hora (pdmtime) em que um fornecedor externo é esperado para atender a essa ocorrência.
service_num	issue.service_num: Campo de texto para documentar um serviço de fornecedor externo ou número da ordem de compra.
product	issue.product: um cursor para um registro na tabela product, que indica o produto afetado por essa ocorrência. issue.product = product.id
ações	issue.actions: Campo de texto grande para documentação das ações.
type_of_contact	issue.type_of_contact: um cursor para um registro na tabela toc, que indica uma categorização geral da perspectiva da ocorrência de affected_end_user. issue.type_of_contact = toc.id
reporting_method	issue.reporting_method: um cursor para um registro na tabela repmeth, que classifica a origem da ocorrência e é selecionado pela pessoa que está criando a ocorrência. issue.reporting_method = repmeth.id
person_contacting	issue.person_contacting: um cursor para um registro na tabela perscon, que indica a função do affected_end_user ou solicitante. issue.person_contacting = perscon.id
status_name	issstat.sym: A descrição do status como visto por um usuário. issue.status = issstat.code
priority_num	pri.sym: a descrição da prioridade como vista por um usuário. issue.priority = pri.enum
category_name	isscat.sym: O nome da categoria de ocorrência como visto por um usuário. issue.category = isscat.code
organization_name	ca_organization.org_name: o nome de uma organização como vista por um usuário. issue.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: o sobrenome do usuário final afetado. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: o nome do usuário final afetado. issue.affected_end_user = ca_contact.contact_uuid

Campo	Observações
affected_end_user_middlename	ca_contact.middle_name: o nome do meio do usuário final afetado. issue.affected_end_user = ca_contact.contact_uuid
assignee_lastname	ca_contact.last_name: o sobrenome do responsável. issue.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: o nome do responsável. issue.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: o nome do meio do responsável. issue.assignee = ca_contact.contact_uuid
groupID	View_Group.contact_uuid: uma representação binária da ID interna usada para o grupo atribuído a essa ocorrência. issue.group_id = ca_contact.contact_uuid
group_name	View_Group.last_name: O nome do grupo atribuído a essa ocorrência. issue.group = ca_contact.contact_uuid
service_type	srv_desc.sym: O nome do tipo de serviço aplicado a essa ocorrência. issue.support_lev = srv_desc.code
impact_num	impact.sym: a descrição do impacto como vista pelos usuários. issue.impact = impact.enum
product_sym	product.sym: a descrição do produto como vista pelos usuários. issue.product = product.id
type_of_contact_sym	toc.sym: A descrição do Tipo de contato como vista pelos usuários. issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: a descrição do Método de relatar conforme vista pelos usuários. issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: a descrição do Contato responsável conforme vista pelos usuários. issue.person_contacting = perscon.id
created_via_sym	interface.sym: issue.created_via = interface.id.
rootcause_sym	rootcause.sym: issue.rootcause = rootcause.id.

View_Issue_Act_Log

A seguir, uma exibição básica de todos os logs de atividades da ocorrência. Essa é uma exibição da tabela activity log (issalg) unida com a tabela activity type (act_type) e a tabela Contato (ca_contact) para fornecer dados mais significativos, como o tipo de atividade real e o nome completo do analista que executou a atividade.

Campo	Observações
id	issalg.id: o identificador exclusivo para este registro na tabela issalg.
persid	issalg.persid: o identificador exclusivo para este registro na tabela issalg, precedido pelo identificador de objeto (issalg para issalg) e dois pontos.
issue_id	issalg.issue_id: o cursor para a id da ocorrência à qual esta atividade pertence. issalg.issue_id = issalg.id
last_mod_dt	issalg.last_mod_dt: A última data/horário de modificação (pdmtime).
time_spent	issalg.time_spent: A duração do tempo gasto nesta atividade, armazenada como o número total de segundos. Por exemplo, 80 = 1 minuto, 20 segundos.
time_stamp	issalg.time_stamp: a data/horário, que pode ser modificada pelo usuário, da atividade (pdmtime).
system_time	issalg.system_time: a data/horário da criação do registro (pdmtime).
analista	issalg.analyst: um identificador binário exclusivo que faz referência à uuid do contato para obter o analista que executou a atividade. issalg.analyst = ca_contact.contact_uuid
descrição	issalg.description: a descrição do texto desta atividade, que pode ser modificada pelo usuário.
action_desc	issalg.action_desc: a descrição de texto da ação automatizada, que não pode ser modificada pelo usuário.
tipo	issalg.type: o cursor de texto para um registro na tabela de tipo de atividade. issalg.type = act_type.code
interno	issalg.internal: o sinalizador inteiro (1 ou 0), que indica se a entrada do log deve ser vista por todos ou se é apenas para uso interno.

Campo	Observações
knowledge_session	issalg.knowledge_session: um identificador para uma determinada sessão de um determinado usuário.
knowledge_tool	issalg.knowledge_tool: um indicador da ferramenta de conhecimento usado para a pesquisa, tal como NLS_FAQ ou EXPERT, etc.
analyst_lastname	View_Contact_Full.last_name: o sobrenome do analista, derivado de issalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: o nome do analista.
analyst_middlename	View_Contact_Full.middle_name: o nome do meio do analista.
activity_type	act_type.sym: tipo de atividade mencionado por issalg.type = act_type.code.

View_Issue_to_Assets

A lista de campos a seguir é uma exibição básica das ocorrências e seus ativos. A tabela de ocorrências (issue) está indiretamente unida à tabela de recursos proprietários (ca_owned_resource) e a outras tabelas relacionadas a ativos para receber uma lista dos ativos de cada ocorrência. Talvez não liste todas as ocorrências, especialmente as que não têm ativos.

Campo	Observações
View_Issue.*	A exibição View_Issue que define todos os campos listados na exibição View_Issue.
assetID	ca_owned_resource.own_resource_uuid: o campo binário que serve como o identificador exclusivo inalterável e interno de um registro de ativo.
asset_serial_num	ca_owned_resource.serial_number: o número de série de um registro de ativo.
asset_class	ca_resource_class.name: uma descrição breve da classe à qual um ativo pertence. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: a família de ativos à qual o ativo pertence. ca_owned_resource.resource_class = ca_resource_class.id E ca_resource_class.family_id = ca_resource_family.id

Campo	Observações
asset_name	ca_owned_resource.resource_name: o nome de rede pelo qual o ativo é conhecido.

View_Issue_to_Issue_Act_Log

A seguir, uma exibição básica de todas as ocorrências e os logs de atividades que as acompanham. Essa exibição une a exibição View_Issue à exibição View_Issue_Act_Log para fornecer informações detalhadas sobre as ocorrências e seus logs de atividades. Os dados reais estão no final da lista de campos.

Campo	Observações
View_Issue.*	Faça referência à exibição View_Issue definida anteriormente neste documento.
issalg_id	issalg.id: o identificador exclusivo para este registro na tabela issalg.
issalg_persid	issalg.persid: o identificador exclusivo para este registro na tabela issalg, precedido pelo identificador de objeto (issalg para issalg) e dois pontos.
issue_id	issalg.issue_id: o cursor para a id da ocorrência à qual esta atividade pertence. issalg.issue_id = issalg.id
issalg_last_mod_dt	issalg.last_mod_dt: a última data/horário de modificação (pdmtime).
time_spent	issalg.time_spent: a duração do tempo gasto nesta atividade, armazenada como o número total de segundos. Por exemplo, 80 = 1 minuto, 20 segundos.
time_stamp	issalg.time_stamp: a data/horário, que pode ser modificada pelo usuário, da atividade (pdmtime).
system_time	issalg.system_time: a data/horário da criação do registro (pdmtime).
analista	issalg.analyst: o cursor binário exclusivo para a uuid de contato para obter o analista que realizou a atividade. issalg.analyst = ca_contact.contact_uuid

Campo	Observações
issalg_description	issalg.description: a descrição do texto desta atividade, que pode ser modificada pelo usuário.
action_desc	issalg.action_desc: a descrição de texto da ação automatizada, que não pode ser modificada pelo usuário.
tipo	issalg.type: o cursor de texto para um registro na tabela de tipo de atividade. issalg.type = act_type.code
interno	issalg.internal: o sinalizador inteiro (1 ou 0), que indica se a entrada do log deve ser vista por todos ou se é apenas para uso interno.
knowledge_session	issalg.knowledge_session: um identificador para uma determinada sessão de um determinado usuário.
knowledge_tool	issalg.knowledge_tool: um indicador da ferramenta de conhecimento usado para a pesquisa, tal como NLS_FAQ ou EXPERT, etc.
issalg_analyst_id	issalg.analyst: o cursor binário exclusivo para a uuid de contato para obter o analista que realizou a atividade. issalg.analyst = ca_contact.contact_uuid

View_Change_to_Request

A seguir, uma exibição básica das requisições de mudança que têm apenas solicitações atribuídas. Essa exibição é resultado da exibição View_Change unida com a tabela request (call_req) para fornecer detalhes sobre a requisição de mudança e sua solicitação associada.

Campo	Observações
View_Change.*	Mostra todos os campos listados na exibição View_Change definida anteriormente neste documento.
cr_id	call_req.id: o identificador exclusivo para registro na tabela call_req.
ref_num	call_req.ref_num: este é um número de referência de solicitação que é usado por analistas e clientes para fazer referência a uma determinada Solicitação.

Campo	Observações
cr_summary	call_req.summary: uma breve descrição da solicitação para referência rápida.
cr_persid	call_req.persid: um identificador exclusivo para este registro na tabela call_req, precedido pelo identificador de objeto (cr para a tabela call_req) e dois pontos.
cr_description	call_req.description: a descrição longa de uma solicitação, conforme ditada por um analista ou cliente.
cr_status	call_req.status: um identificador exclusivo que faz referência a um registro na tabela cr_stat. Indica o status dessa solicitação: call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag: o sinalizador Inteiro usado para determinar se esse registro de solicitação está ativo (1 ou 0).
time_spent_sum	call_req.time_spent_sum: o total derivado de todos os campos time_spent de registros act_log, armazenado em segundos (ou seja, 80 = 1 minuto e 20 segundos).
cr_open_date	call_req.open_date: o carimbo de data/hora da criação da Solicitação (pdmtime).
cr_last_mod_dt	call_req.last_mod_dt: o carimbo de data/hora modificado por último (pdmtime).
cr_close_date	call_req.close_date: o carimbo de data/hora de quando a solicitação foi definida como inativa (pdmtime).
cr_log_agent	call_req.log_agent: um identificador binário exclusivo que faz referência à tabela ca_contact. Faz referência à pessoa que foi o criador original da solicitação. call_req.log_agent = ca_contact.contact_uuid
cr_group_id	call_req.group_id: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa o grupo atualmente atribuído à solicitação. call_req.group_id = ca_contact.contact_uuid
cr_assignee	call_req.assignee: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa a pessoa atualmente atribuída à solicitação. call_req.assignee = ca_contact.contact_uuid

Campo	Observações
cliente	call_req.customer: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa o usuário final afetado para esta solicitação. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: um campo de texto disponível para uso como indicador de jargão contábil para ponderar essa solicitação no centro de custo apropriado
affected_rc	call_req.affected_rc: um identificador binário exclusivo que faz referência a uma linha na tabela ca_owned_resource. Representa o ativo ao qual essa solicitação se aplica. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev: um cursor para um registro de service desk, que automatiza algumas restrições sob as quais esta solicitação deve ser concluída. call_req.support_lev = srv_desc.code
cr_category	call_req.category: este é um identificador exclusivo que faz referência a um registro na tabela prob_ctg. Representa a categoria a qual essa solicitação se aplica. call_req.category = prob_ctg.persid
solução	call_req.solution: um cursor para uma resolução de chamada para obter a solução. call_req.solution = crsol.persid
cr_impact	call_req.impact: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela impact. Indica o escopo que essa solicitação está afetando. call_req.impact = impact.enum
cr_priority	call_req.priority: um identificador exclusivo de número inteiro que faz referência a um registro na tabela pri. Indica como os analistas darão prioridade ao trabalho associado a essa solicitação. call_req.priority = pri.enum
urgency	call_req.urgency: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela urgncy. Documenta o sentimento do usuário de urgência para ter a solicitação resolvida. call_req.urgency = urgncy.enum

Campo	Observações
severity	call_req.severity: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela severity. Indica a gravidade das conseqüências dessa solicitação não resolvida. call_req.severity = sevrty.enum
extern_ref	Especifica um ticket associado.
last_act_id	É a ID da última atividade.
cr_tticket	É um ponteiro para um ticket de problema para obter o ticket associado.
cr_parent	call_req.parent: um cursor de persid para outra persid de solicitação, que facilita a criação de uma hierarquia das requisições de mudança. call_req.parent = call_req.persid
cr_template_name	call_req.template_name: um valor de texto, que indica que esta solicitação é designada para e pode ser escolhida a partir de uma lista como modelo para outras solicitações similares. cr_template.template = call_req.persid
cr_sla_violation	call_req.sla_violation: um número inteiro que conta o número de vezes que os slas anexados a esta solicitação foram violados.
cr_predicted_sla_viol	call_req.predicted_sla_viol: (r5.5) Campo relacionado à tecnologia Neugent.
cr_created_via	call_req.created_via: um cursor de número inteiro para um registro na tabela interface. Indica a partir de qual interface a requisição de mudança foi originada. call_req.created_via = interface.id
cr_call_back_date	call_req.call_back_date: um campo de carimbo de data/hora (pdmtime) que indica uma data/hora no futuro em que o affected_end_user deverá ser contatado.
cr_call_back_flag	call_req.call_back_flag: um indicador Booleano exibido como caixa de seleção ao usuário, indicando se deve ou não notificar o analista na call_req.call_back_date.
event_token	call_req.event_token: usado pelo CA NSM para correspondência de mensagem.
tipo	call_req.type: um campo de texto que faz referência a um registro na tabela crt. Indica o tipo de ITIL dessa solicitação. call_req.type = crt.code
cr_string1	É uma seqüência definida pelo usuário.

Campo	Observações
cr_string2	É uma seqüência definida pelo usuário.
cr_string3	É uma seqüência definida pelo usuário.
cr_string4	É uma seqüência definida pelo usuário.
cr_string5	É uma seqüência definida pelo usuário.
cr_string6	É uma seqüência definida pelo usuário.
change	call_req.change: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela chg Indica a requisição de mudança que foi criada em conseqüência dessa solicitação. call_req.change = chg.id.

View_Issue_to_Issue_WF

Essa exibição é um resultado da exibição View_Change unida à tabela workflow task (wf) para oferecer uma exibição básica da requisição de mudança e suas tarefas de fluxo de trabalho. Isso pode não listar todas as ocorrências, especialmente se não houver tarefas de fluxo de trabalho atribuídas a elas.

Campo	Observações
View_Issue.*	Consulte a definição de View_Issue, anteriormente neste documento, para obter uma descrição de cada campo.
wf_id	isswf.id: um identificador exclusivo para um registro na tabela isswf.
wf_persid	isswf.persid: um identificador exclusivo para esse registro na tabela isswf, precedido pelo identificador de objeto (isswf) e dois pontos.
del	isswf.del: um indicador booleano para determinar se esse registro deve ou não ser exibido ao usuário.
object_type	isswf.object_type: o nome de fábrica usado para identificar o tipo de registro (por exemplo, iss) para o qual essa tarefa de fluxo de trabalho está anexada.
object_id	isswf.object_id: um identificador exclusivo usado para identificar o registro específico ao qual essa tarefa de fluxo de trabalho está anexada. isswf.object_id = issue.id

Campo	Observações
tarefa	isswf.task: um identificador que se refere ao tipo de tarefa que esse registro representa. isswf.task = tskty.code
wf_template	isswf.wf_template: um identificador que faz referência a partir de qual modelo esse registro de tarefa de fluxo de trabalho foi criado. isswf.wf_template = wftpl.id
seqüência	isswf.sequence: um número inteiro que indica a ordem na qual esse registro de tarefa de fluxo de trabalho específico deve ser exibido e executado pelo CA SDM (por exemplo, Ascendente).
wf_status	isswf.status: um identificador que faz referência a um registro tskstat. Indica o status atual desta tarefa de fluxo de trabalho. isswf.status = tskstat.code
group_task	isswf.group_task: um booleano, que indica se essa tarefa pertence a um grupo.
ativo	isswf.asset: um identificador binário exclusivo que faz referência a um registro na tabela ca_owned_resource. isswf.asset = ca_owned_resource.own_resource_uuid
criador	isswf.creator: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Indica a pessoa que criou essa tarefa de fluxo de trabalho. isswf.creator = ca_contact.contact_uuid
date_created	isswf.date_created: a data/carimbo de data e hora na qual essa tarefa de fluxo de trabalho foi criada (pdmtime).
wf_assignee	isswf.assignee: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Indica a pessoa que está atribuída atualmente a essa tarefa de fluxo de trabalho. isswf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by: este é um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Indica a pessoa que concluiu ou aprovou essa tarefa de fluxo de trabalho. isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: o carimbo de data/hora em que a tarefa de fluxo de trabalho passou para um status ativo (pdmtime).

Campo	Observações
wf_est_comp_date	isswf.est_comp_date: o carimbo de data/hora (pdmtime) que indica quando os usuários acreditam que essa tarefa será concluída.
est_duration	isswf.est_duration: a duração estimada para essa tarefa de fluxo de trabalho.
completion_date	isswf.completion_date: o carimbo de data/hora (pdmtime) que indica quando essa tarefa de fluxo de trabalho foi concluída.
actual_duration	isswf.actual_duration: a quantia real de tempo que levou para concluir essa tarefa de fluxo de trabalho.
wf_est_cost	isswf.est_cost: o custo estimado para essa tarefa de fluxo de trabalho
custo	isswf.cost: o custo real exigido para concluir essa tarefa de fluxo de trabalho.
wf_description	isswf.description: uma descrição da tarefa do fluxo de trabalho.
wf_last_mod_dt	isswf.last_mod_dt: o carimbo de data/hora (pdmtime) que indica quando essa tarefa de fluxo de trabalho foi alterada pela última vez.
wf_last_mod_by	isswf.last_mod_by: um identificador binário exclusivo que faz referência a um registro na tabela contact. Indica a última pessoa que fez mudanças nessa tarefa de fluxo de trabalho. isswf.last_mod_by = ca_contact.contact_uuid

View_Issue_to_Properties

Essa exibição é um resultado da exibição de View_Issue unida à tabela issue properties (issprp) para fornecer uma exibição básica das ocorrências e suas propriedades atribuídas. Talvez não liste todas as ocorrências, especialmente se não houver propriedades atribuídas a elas.

Campo	Observações
View_Issue.*	Consulte a definição de View_Issue, anteriormente neste documento, para obter uma descrição de cada campo.
prp_id	issprp.id: um identificador de número inteiro exclusivo para o registro de propriedade.
prp_persid	issprp.persid: um identificador exclusivo para esse registro na tabela prp, precedido pelo identificador de objeto (prp) e dois pontos.
seqüência	issprp.sequence: um número inteiro que indica a ordem na qual esse registro de propriedade particular deve ser exibido pelo CA SDM (por exemplo, Ascendente.)
rótulo	issprp.label: uma descrição curta sobre o que deve ser colocado no campo issprp.value.
valor	issprp.value: um valor inserido pelo usuário em resposta aos campos prp_description e issprp.label
prp_last_mod_dt	issprp.last_mod_dt: o carimbo de data/hora (pdmtime) que indica quando essa propriedade foi modificada pela última vez.
prp_last_mod_by	issprp.last_mod_by: um identificador binário que faz referência a um registro na tabela ca_contact. Representa a pessoa que fez a última modificação nesse registro. issprp.last_mod_by = ca_contact.contact_uuid
obrigatório	issprp.required: este é um Booleano que indica se essa propriedade deve ter um issprp.value antes de o registro ser salvo.
exemplo	issprp.sample: este é um campo de texto que exibe valores de exemplo para guiar o usuário, inserindo o valor mais útil em issprp.value.
owning_iss	issprp.owning_iss: este é um identificador exclusivo usado para identificar o registro específico ao qual essa propriedade está anexada. issprp.object_id = issue.persid
prp_description	issprp.description: um campo de texto que explica o tipo de valor que deve ser inserido em issprp.value.

View_Request

A seguir, uma exibição básica de todas as solicitações. Aqui, a tabela Request foi unida a outras tabelas do CA SDM para fornecer informações mais específicas, como o tipo de serviço de solicitação, gravidade, urgência, categoria e prioridade. Também há alguma informação adicional sobre a solicitação listada. Todos os campos da tabela Request (call_req) estão selecionados. Os campos extraídos que são um resultado das tabelas unidas estão listados no final desta lista de campos.

Campo	Observações
id	call_req.id: o identificador exclusivo para registro na tabela call_req.
persid	call_req.persid: um identificador exclusivo para este registro na tabela call_req, precedido pelo identificador de objeto (cr para a tabela call_req) e dois pontos.
ref_num	call_req.ref_num: este é um número de referência de solicitação que é usado por analistas e clientes para fazer referência a uma determinada Solicitação.
summary	call_req.summary: uma breve descrição da solicitação para referência rápida.
descrição	call_req.description: a descrição longa de uma solicitação, conforme ditada por um analista ou cliente.
status	call_req.status: um identificador exclusivo que faz referência a um registro na tabela cr_stat. Indica o status dessa solicitação. call_req.status = cr_stat.code
active_flag	call_req.active_flag: o sinalizador inteiro para determinar se esse registro de solicitação está ativo (1 ou 0).
open_date	call_req.open_date: o carimbo de data/hora da criação da Solicitação (pdmtime).
time_spent_sum	call_req.time_spent_sum: este é o total derivado de todos os campos time_spent de registros act_log, armazenado em segundos (ou seja, 80 = 1 minuto e 20 segundos).
last_mod_dt	call_req.last_mod_dt: o carimbo de data/hora modificado por último (pdmtime).

Campo	Observações
close_date	call_req.close_date: este é o carimbo de data/hora de quando a solicitação foi definida como inativo (pdmtime).
resolve_date	É a data de quando a solicitação foi resolvida (pdmtime).
rootcause	É um ponteiro para rootcause.id.
log_agent	call_req.log_agent: um identificador binário exclusivo que faz referência à tabela ca_contact. Faz referência à pessoa que foi o criador original da solicitação. call_req.log_agent = ca_contact.contact_uuid
responsável	call_req.assignee: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa a pessoa atualmente atribuída à solicitação. call_req.assignee = ca_contact.contact_uuid
group_id	call_req.group_id: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa o grupo atualmente atribuído à solicitação. call_req.group_id = ca_contact.contact_uuid
cliente	call_req.customer: um identificador binário exclusivo que faz referência a um registro na tabela ca_contact. Representa o usuário final afetado para esta solicitação. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: um campo de texto disponível para uso como indicador de jargão contábil para ponderar essa solicitação no centro de custo apropriado
affected_rc	call_req.affected_rc: um identificador binário exclusivo que faz referência a uma linha na tabela ca_owned_resource. Representa o ativo ao qual essa solicitação se aplica. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
support_lev	call_req.support_lev: um cursor para um registro de service desk, que automatiza algumas restrições sob as quais esta solicitação deve ser concluída. call_req.support_lev = srv_desc.code.

Campo	Observações
categoria	call_req.category: um identificador exclusivo que faz referência a um registro na tabela prob_ctg. Representa a categoria a qual essa solicitação se aplica. call_req.category = prob_ctg.persid
solução	call_req.solution: um cursor para uma resolução de chamada para obter a solução. call_req.solution = crsol.persid
impact	call_req.impact: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela impact. Indica o escopo do impacto da solicitação. call_req.impact = impact.enum
priority	call_req.priority: um identificador exclusivo de número inteiro que faz referência a um registro na tabela pri. Indica como os analistas darão prioridade ao trabalho associado a essa solicitação. call_req.priority = pri.enum
urgency	call_req.urgency: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela urgency. Indica o sentimento de urgência do usuário para ter a solicitação resolvida. call_req.urgency = urgncy.enum
severity	call_req.severity: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela severity. Indica a gravidade das conseqüências dessa solicitação não resolvida. call_req.severity = sevrty.enum
extern_ref	É uma referência externa a um ticket associado.
last_act_id	Identifica a ID da última atividade.
cr_tticket	É um ponteiro para um ticket de problema para obter o ticket associado.
pai	call_req.parent: um cursor de ersid para outra persid de solicitação, que facilita a criação de uma hierarquia das requisições de mudança. call_req.parent = call_req.persid

Campo	Observações
template_name	call_req.template_name: um valor de texto, que indica que esta solicitação é designada para e pode ser escolhida a partir de uma lista como modelo para outras solicitações similares. cr_template.template = call_req.persid
sla_violation	call_req.sla_violation: este é um número inteiro que conta o número de vezes que os slas anexados a esta solicitação foram violados.
predicted_sla_viol	Especifica que uma solicitação foi prevista por neugents com probabilidade de violar o SLA.
macro_predicted_violation	Indica que a solicitação foi prevista por neugents com probabilidade de violar o SLA.
created_via	call_req.created_via: um cursor de número inteiro para um registro na tabela interface que indica de qual interface a requisição de mudança se originou. call_req.created_via = interface.id
call_back_date	call_req.call_back_date: um campo de carimbo de data/hora (pdmtime) que indica uma data/hora no futuro em que o affected_end_user deverá ser contatado.
call_back_flag	call_req.call_back_flag: um indicador Booleano exibido como caixa de seleção ao usuário, indicando se deve ou não notificar o analista na call_req.call_back_date.
event_token	call_req.event_token: usado pelo CA NSM para correspondência de mensagem.
sched_token	call_req.sched_token: usado pelo CA NSM para correspondência de mensagens.
tipo	call_req.type: um campo de texto que faz referência a um registro na tabela crt. Indica o tipo de ITIL dessa solicitação. call_req.type = crt.code
seqüência de caracteres1	É uma seqüência definida pelo usuário.
seqüência de caracteres2	É uma seqüência definida pelo usuário.

Campo	Observações
seqüência de caracteres3	É uma seqüência definida pelo usuário.
seqüência de caracteres4	É uma seqüência definida pelo usuário.
seqüência de caracteres5	É uma seqüência definida pelo usuário.
seqüência de caracteres6	É uma seqüência definida pelo usuário.
problem	É um problema de ITIL.
incident_priority	É uma prioridade do incidente de ITIL.
change	call_req.change: um identificador exclusivo de número inteiro que faz referência a uma linha na tabela chg. Indica a requisição de mudança que foi criada em conseqüência dessa solicitação. call_req.change = chg.id.
service_type	srv_desc.sym: indica o Tipo de serviço real. call_req.support_lev = srv_desc.code
severity_num	sevrty.sym: o número de Gravidade real. call_req.severity = sevrty.enum
urgency_num	urgncy.sym: indica o número de Urgência real. call_req.urgency = urgncy.enum
category_name	prob_ctg.sym: a Área de solicitação real (categoria de problema). call_req.category = prob_ctg.id
ativo	ca_owned_resource.resource_name: o nome do Ativo real. call_req.affected_rc = ca_owned_resource.own_resource_uuid
impact_num	impact.sym: o número de Impacto real. call_req.impact = impact.enum
assignee_lastname	ca_contact.last_name: o sobrenome do Responsável real. call_req.assignee = ca_contact.contact_uuid

Campo	Observações
assignee_firstname	ca_contact.first_name: este é o nome do Responsável real. call_req.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: o nome do meio do Responsável real. call_req.assignee = ca_contact.contact_uuid
customer_lastname	ca_contact.last_name: o sobrenome real do Usuário final afetado. call_req.customer = ca_contact.contact_uuid
customer_firstname	ca_contact.first_name: o nome real do Usuário final afetado. call_req.customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name: o nome do meio real do Usuário final afetado. call_req.customer = ca_contact.contact_uuid
group_name	View_Group.last_name: o nome do Grupo real.
GroupID	View_Group.contact_uuid: a ID chave do Grupo real.
status_name	cr_stat.sym: o status real.
priority_num	pri.sym: o número de Prioridade real.

View_Request_to_Act_Log

A seguir, uma exibição básica de todas as solicitações com seus logs de atividades. A exibição View_Request é unida à exibição View_Act_Log para dar informações mais detalhadas sobre cada atividade por solicitação.

Campo	Observações
View_Request.*	Faça referência ao campo definido na seção View_Request anterior neste documento.
View_Act_Log.*	Faça referência aos campos definidos na seção View_Act_Log anterior neste documento.

View_Request_to_Properties

A seguir, uma exibição básica das solicitações de chamada e suas propriedades. Essa exibição listas toda a tabela call request (call_req) e a tabela request property (cr_prp).

Campo	Observações
View_Request.*	Faça referência aos campos definidos na seção View_Request deste documento.
crprp_id	cr_prp.id: um identificador de número inteiro exclusivo para o registro de propriedade.
crprp_persid	cr_prp.persid: um identificador exclusivo para esse registro na tabela cr_prp, precedido pelo identificador de objeto (cr_prp) e dois pontos.
seqüência	cr_prp.sequence: um número inteiro que indica a ordem na qual esse registro de propriedade particular deve ser exibido pelo CA SDM (por exemplo, Ascendente.)
rótulo	cr_prp.label: uma descrição curta sobre o que deve ser colocado no campo cr_prp.value.
valor	cr_prp.value: um valor inserido pelo usuário em resposta aos campos prp_description e cr_prp.label.
crprp_last_mod_dt	cr_prp.last_mod_dt: o carimbo de data/hora (pdmtime) que identifica quando essa propriedade foi modificada pela última vez.
crprp_last_mod_by	cr_prp.last_mod_by: um identificador binário que faz referência a um registro na tabela ca_contact. Representa a pessoa que fez a última modificação nesse registro. cr_prp.last_mod_by = ca_contact.contact_uuid
obrigatório	cr_prp.required: um booleano indicando se essa propriedade deve ter um cr_prp.value antes de o registro ser salvo.
exemplo	cr_prp.sample: um campo de texto que exibe valores de exemplo para guiar o usuário, inserindo o valor mais útil em cr_prp.value.
owning_cr	cr_prp.owning_cr: o identificador exclusivo usado para identificar o registro específico ao qual essa propriedade está anexada. cr_prp.object_id = call_req.persid

Campo	Observações
crprp_description	cr_prp.description: um campo de texto que explica o tipo de valor que deve ser inserido em cr_prp.value.

Apêndice B: RFC 2251 Códigos de resultados de LDAP

Esta seção contém os seguintes tópicos:

Códigos de retorno do LDAP (na página 1133)
Códigos de retorno do servidor LDAP (na página 1133)
Códigos de retorno do cliente LDAP (na página 1139)
Padrões de RFC associados ao LDAP (na página 1141)

Códigos de retorno do LDAP

O LDAP tem um conjunto de códigos de resultado de operação que pode ser gerado pelo servidor LDAP em resposta a várias solicitações de LDAP. Esses códigos indicam o status da operação de protocolo e são categorizados de acordo com as categorias de código de retorno do cliente ou servidor.

Códigos de retorno do servidor LDAP

A tabela a seguir lista os códigos de retorno do servidor:

Hexadecimal	Decimal	Descrição
0x00	0	LDAP_SUCCESS Indica a operação solicitada do cliente concluída com êxito.
0x01	1	LDAP_OPERATIONS_ERROR Indica que ocorreu um erro interno. O servidor é incapaz de responder com um erro mais específico, e não pode responder corretamente a uma solicitação. Isso não indica que o cliente enviou uma mensagem incorreta.
0x02	2	LDAP_PROTOCOL_ERROR Indica que o servidor recebeu uma solicitação inválida ou malformada do cliente.

Hexadecimal	Decimal	Descrição
0x03	3	LDAP_TIMELIMIT_EXCEEDED Indica que o tempo limite da operação especificado pelo cliente ou servidor foi excedido. Em operações de pesquisa, são retornados resultados incompletos.
0x04	4	LDAP_SIZELIMIT_EXCEEDED Indica que em uma operação de pesquisa, o limite de tamanho especificado pelo cliente ou servidor foi excedido. São retornados resultados incompletos.
0x05	5	LDAP_COMPARE_FALSE Não indica uma condição de erro. Indica que os resultados de uma operação de comparação são falsos.
0x06	6	LDAP_COMPARE_TRUE Não indica uma condição de erro. Indica que os resultados de uma operação de comparação são verdadeiros.
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED Indica que durante uma operação de vinculação o cliente solicitou um método de autenticação não suportado pelo servidor LDAP.
0x08	8	LDAP_STRONG_AUTH_REQUIRED Indica um dos seguintes: ■ Em solicitações de vinculação, o servidor LDAP aceita apenas uma autenticação forte. ■ Em uma solicitação de cliente, o cliente solicitou uma operação, como excluir, que exige uma autenticação forte. ■ Em um aviso não solicitado de desconexão, o servidor LDAP descobre que a segurança que está protegendo a comunicação entre o cliente e servidor falhou inesperadamente ou está comprometida.
0x09	9	Reservado.
0x0A	10	LDAP_REFERRAL Não indica uma condição de erro. Em LDAPv3, indica que o servidor não mantêm a entrada de destino da solicitação, mas que os servidores no campo de referência podem.
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED Indica que um limite de servidor LDAP definido por uma autoridade administrativa foi excedido.

Hexadecimal	Decimal	Descrição
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION Indica que o servidor LDAP era incapaz de satisfazer uma solicitação uma vez que uma ou mais extensões críticas não estavam disponíveis. Ou o servidor não oferece suporte ao controle ou o controle não é apropriado para o tipo de operação.
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED Indica que a sessão não está protegida por um protocolo, como TLS (Transport Layer Security), que fornece confidencialidade de sessão.
0x0E	14	LDAP_SASL_BIND_IN_PROGRESS Não indica uma condição de erro, mas indica que o servidor está pronto para a próxima etapa do processo. O cliente deve enviar ao servidor o mesmo mecanismo SASL para que o processo continue.
0x0F	15	Não usado.
0x10	16	LDAP_NO_SUCH_ATTRIBUTE Indica que o atributo especificado na operação modificar ou comparar não existe na entrada.
0x11	17	LDAP_UNDEFINED_TYPE Indica que o atributo especificado na operação modificar ou adicionar não existe no esquema do servidor LDAP.
0x12	18	LDAP_INAPPROPRIATE_MATCHING Indica que a regra correspondente especificada no filtro de pesquisa não coincide com uma regra definida para a sintaxe do atributo.
0x13	19	LDAP_CONSTRAINT_VIOLATION Indica que o valor de atributo especificado em uma operação de modificação, adição ou de modificação de DN viola as restrições colocadas no atributo. A restrição pode ser de tamanho ou conteúdo (apenas de seqüência, não binária).
0x14	20	LDAP_TYPE_OR_VALUE_EXISTS Indica que o valor de atributo especificado em uma operação de modificação ou adição já existe como um valor para esse atributo.
0x15	21	LDAP_INVALID_SYNTAX Indica que o valor de atributo especificado em uma operação de adição, comparação ou modificação está em uma sintaxe não reconhecida ou inválida para o atributo.
	22-31	Não usado.

Hexadecimal	Decimal	Descrição
0x20	32	LDAP_NO_SUCH_OBJECT Indica que o objeto de destino não pode ser encontrado. Esse código não é retornado nas seguintes operações: ■ Operações de pesquisa que encontram a base de pesquisa, mas não podem encontrar nenhuma entrada que corresponda ao filtro de pesquisa. ■ Vincular operações
0x21	33	LDAP_ALIAS_PROBLEM Indica que ocorreu um erro quando foi retirada a referência de um alias.
0x22	34	LDAP_INVALID_DN_SYNTAX Indica que a sintaxe do DN é incorreta. No entanto, se a sintaxe de DN estiver correta, mas as regras de estrutura do servidor LDAP não permitirem a operação, o servidor retornará: LDAP_UNWILLING_TO_PERFORM
0x23	35	LDAP_IS_LEAF Indica que a operação especificada não pode ser executada em uma entrada de folha. (Esse código não está atualmente nas especificações de LDAP, mas está reservado para essa constante.)
0x24	36	LDAP_ALIAS_DEREF_PROBLEM Indica que, durante uma operação de pesquisa, o cliente não tem direitos de acesso para ler o nome do objeto de alias nem é permitida a retirada de referência.
	37-47	Não usado.
0x30	48	LDAP_INAPPROPRIATE_AUTH Indica que, durante uma operação de vinculação, o cliente tenta usar um método de autenticação que o cliente não pode usar corretamente. Por exemplo, uma dessas opções gera esse erro: ■ O cliente retorna credenciais simples quando as credenciais fortes são exigidas. ■ O cliente retorna um DN e uma senha para um vínculo simples quando a entrada não tem uma senha definida.

Hexadecimal	Decimal	Descrição
0x31	49	LDAP_INVALID_CREDENTIALS Indica que, durante uma operação de vinculação: ■ O cliente passou um DN ou senha incorreta. ■ A senha está incorreta porque expirou; a detecção de intruso bloqueou a conta ou por algum outro motivo semelhante.
0x32	50	LDAP_INSUFFICIENT_ACCESS Indica que o chamador não tem direitos suficientes para executar a operação solicitada.
0x33	51	LDAP_BUSY Indica que o servidor LDAP está muito ocupado para processar a solicitação do cliente no momento, mas se ele esperar e enviar novamente a solicitação, talvez o servidor não possa processá-la.
0x34	52	LDAP_UNAVAILABLE Indica que o servidor LDAP não pode processar a solicitação de vinculação do cliente, normalmente porque ele está sendo encerrado.
0x35	53	LDAP_UNWILLING_TO_PERFORM Indica que o servidor LDAP não pode processar a solicitação por causa das restrições definidas pelo servidor. Esse erro é retornado pelos seguintes motivos: ■ A solicitação para adicionar entrada viola as regras de estrutura do servidor. ■ A solicitação para modificar o atributo especifica atributos que os usuários não podem modificar. ■ As restrições de senha impedem a ação. ■ As restrições de conexão impedem a ação.
0x36	54	LDAP_LOOP_DETECT Indica que o cliente descobriu um alias ou loop de referência e por isso não é possível concluir essa solicitação.
	55-63	Não usado.

Hexadecimal	Decimal	Descrição
0x40	64	LDAP_NAMING_VIOLATION Indica que a operação de adição ou modificação de DN viola as regras de estrutura do esquema. Por exemplo: ■ A solicitação coloca a entrada subordinada a um alias. ■ A solicitação coloca a entrada subordinada a um container que é proibido pelas regras de contenção. ■ O RDN da entrada usa um tipo proibido de atributo.
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Indica que a operação de adição, modificação ou modificação de DN viola as regras de classe de objeto para a entrada. Por exemplo, os seguintes tipos de solicitações retornam esse erro: ■ A operação de adição ou modificação tenta adicionar uma entrada sem um valor para um atributo obrigatório. ■ A operação de adição ou modificação tenta adicionar uma entrada com um valor para um atributo que a definição de classe não contém. ■ A operação de modificação tenta remover um atributo obrigatório sem remover a classe auxiliar que define o atributo, como necessário.
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF Indica que a operação solicitada é permitida apenas em entradas de folha. Por exemplo, os seguintes tipos de solicitações retornam esse erro: ■ O cliente solicita uma operação de exclusão em uma entrada pai. ■ O cliente solicita uma operação de modificação de DN em uma entrada pai.
0x43	67	LDAP_NOT_ALLOWED_ON_RDN Indica que a operação de modificação tentou remover um valor de atributo que forma o nome exclusivo relativo da entrada.
0x44	68	LDAP_ALREADY_EXISTS Indica que a operação de adição tentou adicionar uma entrada que já existe ou que a operação de modificação tentou renomear uma entrada com o nome de uma entrada que já existe.

Hexadecimal	Decimal	Descrição
0x45	69	LDAP_NO_OBJECT_CLASS_MODS Indica que a operação de modificação tentou modificar as regras de estrutura de uma classe de objeto.
0x46	70	LDAP_RESULTS_TOO_LARGE Reservado para CLDAP.
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS Indica que a operação de modificação de DN move a entrada de um servidor LDAP a outro e, assim, exige mais de um servidor LDAP.
	72-79	Não usado.
0x50	80	LDAP_OTHER Indica uma condição de erro desconhecida. Esse é o valor padrão para códigos de erro NDS que não mapeia para outros códigos de erro LDAP.

Códigos de retorno do cliente LDAP

A tabela a seguir lista os códigos de retorno do cliente:

Hexadecimal	Decimal	Descrição
0x51	81	LDAP_SERVER_DOWN Indica que as bibliotecas LDAP não podem estabelecer uma conexão inicial com o servidor LDAP. O servidor LDAP está inativo ou o nome de host especificado ou o número da porta está errado.
0x52	82	LDAP_LOCAL_ERROR Indica que o cliente LDAP tem um erro. Geralmente é uma erro de falha na alocação de memória dinâmica.
0x53	83	LDAP_ENCODING_ERROR Indica que o cliente LDAP encontrou erros ao codificar uma solicitação de LDAP destinada ao servidor LDAP.
0x54	84	LDAP_DECODING_ERROR Indica que o cliente LDAP encontrou erros ao decodificar uma resposta de LDAP do servidor LDAP.

Hexadecimal	Decimal	Descrição
0x55	85	LDAP_TIMEOUT Indica que o prazo do cliente LDAP foi excedido enquanto esperava-se um resultado.
0x56	86	LDAP_AUTH_UNKNOWN Indica que a função ldap_bind ou ldap_bind_s foi chamada com um método de autenticação desconhecido.
0x57	87	LDAP_FILTER_ERROR Indica que a função ldap_search foi chamada com um filtro de pesquisa inválido.
0x58	88	LDAP_USER_CANCELLED Indica que o usuário cancelou a operação de LDAP.
0x59	89	LDAP_PARAM_ERROR Indica que uma função LDAP foi chamada com um valor de parâmetro inválido (por exemplo, o parâmetro de ID é NULL).
0x5A	90	LDAP_NO_MEMORY: Indica que uma função de alocação de memória dinâmica falhou ao chamar uma função LDAP.
0B	91	LDAP_CONNECT_ERROR Indica que o cliente LDAP perdeu sua conexão ou não pôde estabelecer uma conexão ao servidor LDAP.
0x5C	92	LDAP_NOT_SUPPORTED Indica que o cliente não oferece suporte ao suporte solicitado. Por exemplo, se o cliente LDAP estiver estabelecido como um cliente LDAPv2, as bibliotecas definirão esse código de erro quando o cliente solicitar o recurso LDAPv3.
0x5D	93	LDAP_CONTROL_NOT_FOUND Indica que o cliente solicitou um controle que as bibliotecas não podem encontrar na lista de controles suportados enviada pelo servidor LDAP.
0x5E	94	LDAP_NO_RESULTS_RETURNED Indica que o servidor LDAP não enviou nenhum resultado. Quando a função ldap_parse_result é chamada, nenhum código de resultado é incluído na resposta do servidor.

Hexadecimal	Decimal	Descrição
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN Indica que mais resultados são encadeados na mensagem de resultado. As bibliotecas definem esse código quando a chamada à função ldap_parse_result revela que esses códigos de resultado adicionais estão disponíveis.
0x60	96	LDAP_CLIENT_LOOP Indica que as bibliotecas LDAP detectaram um volta. Normalmente, isso acontece ao seguir as referências.
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED Indica que a referência excede o limite de salto. O limite de salto determina por quantos servidores o cliente pode saltar para recuperar os dados. Por exemplo, considere as seguintes condições: ■ O limite de salto é dois. ■ A referência é para o servidor D que pode ser contatado apenas pelo servidor B (1 salto) que contata o servidor C (2 saltos) que contata o servidor D (3 saltos) Com essas condições, o limite de salto é excedido e as bibliotecas LDAP definem esse código.

Padrões de RFC associados ao LDAP

A tabela a seguir descreve os padrões RFC associados a LDAP disponíveis para uso:

RFC	Descrição
1274	COSINE e Internet X.500 Schema
1275	Requisitos de replicação para fornecer um Diretório de Internet usando X.500
1276	Replicação e extensões de Operações distribuídas para fornecer um Diretório de Internet usando X.500
1308	Introdução executiva a serviços de diretório usando o protocolo X.500
1309	Visão geral técnica dos serviços de diretório usando o protocolo X.500
1430	Um plano estratégico para implementar um serviço de diretório X.500 de Internet
1488	Representação da string X.500 das sintaxes de atributo padrão

RFC	Descrição
1558	Uma representação de seqüência de caracteres de filtros de pesquisa LDAP
1617	Diretrizes de nomeação e estrutura de diretórios pilotos X. 500
1777	Lightweight Directory Access Protocol v2
1778	Representação de seqüência de caracteres das sintaxes de atributo padrão
1779	Uma representação de seqüência de caracteres de nomes distintos
1804	Publicação de esquema no Diretório X. 500
1823	A API do LDAP
1959	Um formato de URL LDAP
1960	Uma representação de seqüência de caracteres de filtros de pesquisa LDAP
2044	UTF -8, um formato de transformação de Unicode e ISO 10646
2164	O uso de um Diretório X.500/LDAP para dar suporte ao mapeamento de endereços MIXER
2218	Um esquema comum para o serviço White Pages da Internet
2247	Usando domínios em nomes distintos do LDAP/X.500
2251	Lightweight Directory Access Protocol (v3)
2252	Lightweight Directory Access Protocol (v3): Definições da sintaxe de atributo
2253	Lightweight Directory Access Protocol (v3): Representação da sequência UTF-8 dos nomes distintos
2254	Uma representação de seqüência de caracteres de filtros de pesquisa LDAP
2255	O formato do URL LDAP
2256	Um resumo do esquema do usuário X.500(96) para ser usado com LDAPv3
2279	UTF-8, um formato de transformação de ISO 10646
2293	Representando tabelas e subárvores no diretório X. 500
2294	Representando a hierarquia de endereços O/R na árvore de Informação do Diretório X. 500
2307	Uma abordagem para o uso de LDAP como um serviço NIS (network information service)
2377	Plano de nomenclatura aplicativos de Internet com diretório habilitado
2531	Esquema de recurso de conteúdo para fax via Internet

RFC	Descrição
2559	Protocolos operacionais PKI X.509 - LDAPv2
2587	Esquema PKI X.509 - LDAPv2
2589	Lightweight Directory Access Protocol (v3): Extensões para os Serviços de Diretório Dinâmicos
2596	Uso de códigos de linguagem em LDAP
2649	Controle e esquema de LDAP para assinaturas de operação
2657	RFC 2657 - Cliente LDAPv2 versus malha de índice
2696	Extensão de controle LDAP para manipulação de resultados de página simples
2713	Esquema para representar objetos Java (tm) em um Diretório de LDAP
2714	Esquema para representar referências de objeto CORBA em um Diretório de LDAP
2739	Atributos de calendário de vCard e LDAP
2798	Definição de classe de objeto LDAP de inetOrgPerson
2820	Requisitos de controle de acesso para LDAP
2829	Métodos de autenticação para LDAP
2830	Lightweight Directory Access Protocol (v3): Extensão para Transport Layer Security
2849	LDIF (LDAP data interchange format)
2879	Esquema de recurso de conteúdo para fax via Internet (v2)
2891	Extensão de controle de LDAP para classificação de resultados de pesquisa no servidor
3045	Armazenando informações de fornecedor no DSE raiz de LDAP
3062	Operação estendida de modificação de senha de LDAP
3112	Esquema de senha de autenticação de LDAP
3296	Referências a subordinados nomeados em diretórios LDAP
3377	Lightweight Directory Access Protocol (v3): Especificação técnica
3384	Requisitos de replicação do LDAP (versão 3)

Apêndice C: Comandos de referência

Esse apêndice fornece os comandos de referência detalhados disponíveis para o CA SDM.

Esta seção contém os seguintes tópicos:

bop_sinfo--Exibir informações do sistema (na página 1146)
dbmonitor_nxd--Daemon de monitoramento de banco de dados (na página 1147)
pdm_backup--Gravar banco de dados no arquivo ASCII (na página 1149)
pdm_cache_refresh--Atualizar banco de dados (na página 1151)
pdm_configure--Abrir a janela de configuração (na página 1152)
pdm_d_refresh--Start Failed Daemons (na página 1153)
pdm_deref--Retirar referência dos dados ASCII (na página 1154)
pdm_discimp -- Importação de ativos descobertos (na página 1157)
pdm_discupd -- Atualização do ativo descoberto (na página 1159)
pdm_edit--Configurar processos do servidor (na página 1160)
pdm_extract--Extrair dados do banco de dados (na página 1162)
pdm_halt--Terminar daemons ou parar serviços (na página 1165)
pdm_init--Iniciar daemons (na página 1166)
pdm_key_refresh--Atualizar informações-chave armazenadas em cache (na página 1167)
pdm_lexutil--Modificar o léxico do CA SDM (na página 1167)
pdm_k_reindex — Utilitário de reindexação de documentos de conhecimento (na página 1168)
pdm_listconn--Listar conexões ativas (na página 1172)
pdm_load--Adicionar, atualizar e excluir registros do banco de dados (na página 1175)
pdm_logfile--Alterar o tamanho de cutover de stdlog (na página 1177)
pdm_log4j_config Utility--Modify the log4j properties File (na página 1178)
pdm_proctor_init--Iniciar solicitador em servidores secundários (na página 1184)
pdm_replace--Substituir uma tabela do banco de dados (na página 1184)
pdm_rest_util – Gerenciar o aplicativo serviços web do CA SDM RESTful (na página 1186)
pdm_restore--Restaurar um banco de dados (na página 1187)
pdm_status--Mostrar status de daemons ou processos (na página 1189)

pdm_task--Definir variáveis de ambiente (na página 1189)
pdm_text_cmd--Interface da linha de comando API do texto (na página 1190)
pdm_uconv--Convert Local Charset to UTF-8 (na página 1193)
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)
pdm_webstat--Retornar estatísticas de uso da Web (na página 1199)
relatório--Gerar relatórios (na página 1203)
rpt_srv--Generate Reports (na página 1204)
uniconv--Iniciar o daemon conversor de eventos do CA NSM para UNIX (na página 1206)

bop_sinfo--Exibir informações do sistema

O utilitário bop_sinfo exibe as informações sobre um único objeto Majic definido. Você pode executar esse utilitário em objetos listados no *Guia de Referência Técnica*.

Sintaxe

Esse comando apresenta o seguinte formato:

```
bop_sinfo [-s server] [-p] [-l] [-d] [f] [-q] [-t] [-m] [-a] object [-h]
```

-s server

Especifica o servidor a ser consultado.

-p

Exibe as informações do produtor.

-l

Exibe a lista de domset.

-d

Exibe as informações do objeto do banco de dados, incluindo o nome e o tipo de todos os atributos.

-f

Exibe as informações da fábrica, incluindo o rel_attr e common_name.

-q

Exibe o nome de esquema da tabela associada.

-t

Exibe os gatilhos do objeto.

-m

Exibe os métodos usados pelo objeto.

Uma

Exibe os detalhes de atributo.

object

O nome do objeto a ser consultado

-h

Exibe ajuda no utilitário.

Exemplo: exibição das informações do sistema para o objeto dmn

```
bop_sinfo -d dmn

Factory dmn
 Atributos
    id                  INTEGER
    producer_id LOCAL STRING(20)
    persistent_id       STRING(30)
    sym                 STRING(60) REQUIRED
    delete_flag SREL -> actbool.enum REQUIRED
    desc        STRING(40)
    tables              BREL <- dcon.dom_id {dom_id = ?}
    last_mod            DATE
    last_mod_by SREL -> cnt.id
    audit_useridLOCAL SREL -> cnt.id
```

dbmonitor_nxd--Daemon de monitoramento de banco de dados

O daemon de monitoramento de banco de dados (dbmonitor_nxd) oferece um mecanismo que permite o armazenamento em cache do CA SDM de tabelas de banco de dados específicas para serem atualizadas quando as mudanças forem realizadas externamente do CA SDM.

A função principal do dbmonitor_nxd é gerar notificações CHANGE para mudanças em tabelas especificadas que não ocorreram através do CA SDM. Para desempenhar essa função, o monitor periodicamente consulta o banco de dados, determina o que foi mudado externamente e, então, envia notificações CHANGE para o servidor bpvirtdb_nxd. O servidor bpvirtdb_nxd notifica todos os servidores domsrvr sobre a mudança, o que faz cada domsrvr atualize seu cache dos objetos de banco de dados específicos e, então, notifiquem todos os outros processos que assinam as mudanças nas tabelas especificadas.

Esse mecanismo funciona bem para as mudanças externas ocasionais nas tabelas monitoradas. Entretanto, em casos em que atualizações em massa são realizadas externamente, uma grande quantidade de notificações CHANGE é difundida, o que leva a muitas consultas ao banco de dados a partir de vários processos do CA SDM. Isso tem um impacto significativo sobre o desempenho do CA SDM.

Para eliminar esse impacto no desempenho do CA SDM, o dbmonitor_nxd foi atualizado para essa release do produto. O monitor oferece suporte à interface da linha de comando que permite que o usuário inicie e interrompa o monitoramento das tabelas especificadas.

Sintaxe

Esse comando apresenta o seguinte formato:

```
dbmonitor_nxd  -c <command> -t <tables>
```

<command>

Insira iniciar ou interromper.

<tables>

Especifica o nome da tabela ou uma lista delimitada por vírgula de nomes de tabelas que devem corresponder a uma ou mais tabelas especificadas na variável de ambiente NX_DBMONITOR_TABLES.

Cada solicitação é enviada para o daemon dbmonitor_nxd. O daemon realiza a ação adequada e retorna uma mensagem para o usuário indicando a ação realizada.

- Se uma solicitação de início for invocada para uma tabela que já tenha sido iniciada, nenhuma ação é realizada.
- Se uma solicitação de interrupção for feita para uma tabela que já tenha sido interrompida, nenhuma ação é realizada.
- Se o monitoramento for iniciado ou interrompido com sucesso para uma tabela, também é gravada uma mensagem de log para stdlog.

Observação: quando o monitor é pausado para uma tabela, todos os processos do CA SDM que armazenam dados em cache a partir dessa tabela podem ficar desatualizadas e não é realizado nenhum fornecimento para atualizar esse cache.

Por exemplo, o BOPLGIN armazena em cache os registros de Contato (das tabelas ca_contact e usp_contact) e esse cache não será atualizado se o monitor for pausado para a tabela ca_contact durante o tempo em que as atualizações externas foram carregadas para o banco de dados. No caso do BOPLGIN isso terá uma pequena consequência, pois os principais atributos de Contato armazenados em cache no BOPLGIN são obtidos a partir da tabela usp_contact e não da ca_contact.

Observação: quando o monitor está pausado para uma tabela, os Usuários da web não poderão consultar as mudanças na tabela enquanto estiverem visualizando um formulário de detalhes criado externamente enquanto o monitor estava pausado.

pdm_backup--Gravar banco de dados no arquivo ASCII

pdm_backup pára o CA SDM e, em seguida, grava uma ou mais tabelas de um banco de dados do CA SDM em um arquivo ASCII. Você pode usar esse arquivo de saída como um arquivo de entrada para o pdm_restore. Além do conteúdo do banco de dados, pdm_backup faz backup dos arquivos de configuração do aplicativo.

Se você tiver ferramentas de backup específicas do ambiente operacional, recomendamos usá-las em vez de pdm_backup. Como o pdm_backup é uma ferramenta genérica, ele pode ser lento em algumas combinações de ambientes operacionais.

Observação: como parte de seu processamento, o pdm_backup primeiro encerra os daemons (UNIX) ou os serviços (Windows).

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_backup [-d] [-g] [-v] -f filename [ALL | table1...tableN]
```

-d

Especifica o backup apenas dos dados do banco de dados.

-g

Especifica que é feito backup apenas dos dados que não são do banco de dados. Isso significa que é feito backup apenas das janelas (formulários) e de outros dados que não são do banco de dados.

-v

Especifica modo verboso, que escreve comentários sobre o andamento de comando a stdout.

-f *filename*

Especifica um arquivo de saída.

ALL|table1...tableN

Especifica TODOS os arquivos ou uma ou mais tabelas a serem gravadas. Se mais de uma tabela for especificada, separe cada uma com espaços.

- É possível encontrar os nomes de tabela no arquivo de esquema de banco de dados do CA SDM, ddict.sch, localizado no $NX_ROOT/local (UNIX) ou *diretório de instalação*\site (Windows). $NX_ROOT ou *diretório de instalação* é o diretório em que oCA SDM foi instalado.
- Se nenhuma tabela for especificada, o banco de dados inteiro do CA SDM será gravado, incluindo os grupos de janela e os arquivos de registro de menu.

Restrições

pdm_backup não pode ser executado enquanto o CA SDM estiver ativo.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

Mais informações:

pdm_restore--Restaurar um banco de dados (na página 1187)

pdm_cache_refresh--Atualizar banco de dados

pdm_cache_refresh faz com que os daemons do CA SDM ou os processo usem os dados carregados no banco de dados com pdm_userload ou outros utilitários de banco de dados, incluindo ferramentas de banco de dados que não pertencem ao CA SDM.

A maioria dos daemons do CA SDM e executáveis mantém um cache na memória dinâmica dos registros de banco de dados. O cache melhora o desempenho eliminado a necessidade de acessar o banco de dados quando os dados necessários já estão disponíveis. Os executáveis do CA SDM notificam uns aos outros sobre atualizações no banco de dados, de modo que o cache está sempre atualizado. Contudo, não há nenhuma notificação de atualizações de utilitários externos, tal como pdm_userload ou utilitários de banco de dados de terceiros. Se novos dados forem carregados no banco de dados de uma dessas origens externas, é necessário usar o utilitário pdm_cache_refresh para notificar sobre módulos em execução que seu cache deve ser atualizado a partir do banco de dados.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_cache_refresh [-f filename] [-t tablenamelist] [-d] [-v]
```

-f filename

Especifica um arquivo de texto contendo uma lista de tabelas de banco de dados que foi modificada externamente. O arquivo de texto consiste em uma ou mais linhas, cada linha contendo um ou mais nomes da tabela separados por espaços.

-t tablename

Especifica uma ou mais tabelas que foram modificadas externamente. Se a lista contiver mais de uma tabela, os nomes da tabela devem ser separados por ponto e vírgula e a lista inteira deve estar entre aspas. As tabelas são listadas no apêndice "Dicionário de elementos de dados" no *Guia de Referência Técnica*.

Por exemplo, considere que você carregou os dados de local e site no banco de dados do CA SDM com um utilitário de terceiros. Para indicar aos daemons do CA SDM para atualizar seu cache para essas tabelas, emita o seguinte comando:

```
pdm_cache_refresh -t "Location;Site"
```

-d

Envia uma mensagem ao domsrvr, o servidor de domínios do CA SDM. O servidor de domínios recarrega todas as listas de seleção, fazendo com que quaisquer janelas de listas exibidas em cliente pisquem.

-v

Especifica modo verboso. O valor 1 é o modo breve. O valor 2 imprime as mensagens de andamento no arquivo de log.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_configure--Abrir a janela de configuração

pdm_configure abre uma janela contendo a janela de configuração do CA SDM. Use essa janela para definir a configuração do CA SDM após instalar o CA SDM, ou para alterar a configuração do CA SDM após o CA SDM estar sendo executado. Possíveis motivos para alterar a configuração do CA SDM incluem:

- Alterando o tipo de banco de dados ou servidor
- Recarregar dados padrão
- Alterar senhas para contas de sistema do CA SDM
- Recriar arquivos do esquema para incorporar as mudanças
- Reconfigurar como Servidor primário ou secundário

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_configure
```

Restrições

pdm_configure pode ser executado em um servidor do CA SDM (Primário ou Secundário) ou em um cliente Linux do CA SDM. Você deve ser o usuário privilegiado ou raiz para executar o pdm_configure.

pdm_d_refresh--Start Failed Daemons

O utilitário de linha de comando pdm_d_refresh é usado principalmente para configurações remotas de daemon. Ele diz ao gerenciador daemon para tentar iniciar os daemons que falharam ao iniciar dez vezes e que o gerenciador tenha sinalizado como "não executável". Geralmente isso é causado por iniciar o servidor principal quando uma das seguintes situações ocorrer:

- Um ou mais servidores secundários ainda não tiverem sido iniciados.
- Um servidor secundário é parado enquanto o servidor principal está em execução.

O gerenciador de daemon tenta iniciar os daemons remotos, mas, se não conseguir entrar em contato com o servidor secundário, ele tentará dez vezes e parará. A execução deste utilitário sinaliza todos os daemons como executáveis e redefine o contador de reinício. Em seguida, o gerente de daemon tenta iniciar todos os daemons parados.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_d_refresh
```

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_deref--Retirar referência dos dados ASCII

pdm_deref processa a entrada formatada ASCII para trocar os dados encontrados em uma tabela de banco de dados pelos dados encontrados em outra tabela de banco de dados. Pode ser usado para criar arquivos compatíveis com pdm_userload a partir de uma planilha ou banco de dados que não seja do CA SDM. Também pode ser usado para criar relatórios ou arquivos de saída para uma planilha ou banco de dados que não seja do CA SDM.

Importante: Não use o pdm_deref se não estiver familiarizado com o SQL. Os diretórios " exportação" e "importação" em $NX_ROOT/samples (UNIX) ou diretório de instalação\amostras (Windows) contêm um conjunto padrão de specfiles para exibição.

Sintaxe

Esse comando apresenta o seguinte formato:

```
name pdm_deref –s specfile [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <filename
```

-s specfile

(Obrigatório) Especifica um arquivo que define quais dados são trocados e as condições sob as quais eles são alterados.

Specfile contém uma lista de comandos do SQL no seguinte formato (note que "att" significa atributo e "atts" atributos):

```
Deref

{
input = <lista de atributos "from" do arquivo de entrada>
output = <lista de atributos "to" para o arquivo de entrada>
rule = "SELECT <atributos usados para preencher atributos de saída> \
  FROM <nome da tabela>  \
  WHERE <atributo do nome da tabela para corresponder com a entrada 1> =?\
  AND <atributo do nome da tabela para corresponder com a entrada 2> = ? \
  OR <atributo do nome da tabela para corresponder com a entrada 3> =?"
}
```

-c

Produz uma saída de valores separados por vírgula (CSV), tal como:

```
"field1","field2","field3"
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-e

Produz saída CSV (comma-separated value – valor separado por vírgulas) com aspas duplas atuando como sequência de Escape para aspas duplas incorporadas. Por exemplo:

```
"Texto com uma "sequência entre aspas"".
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-r

Produz saída justificada à esquerda nos formatos se os rótulos de coluna não forem fornecidas no arquivo de entrada:

```
"label":"value"
```

ou

```
"value"
```

Esta opção visa ser usada com impressoras de linhas, por exemplo:

```
Field_Name: Valor do campo
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-d

Produz informações de diagnóstico.

-h

Exibe informações de ajuda e uso.

-n

Especifica que você não deseja tratar as chaves estrangeiras com valor igual a 0 como NULL. Esse argumento deve ser usado apenas sob circunstâncias especiais ao recuperar um banco de dados danificado.

-u

Produz saída sem cabeçalhos.

-v [1|2]

Especifica modo verboso. O valor 1 é o modo breve. O valor 2 imprime as mensagens de andamento no arquivo de log.

filename

(Opcional) Especifica o arquivo de entrada em formato ASCII a ser processado. Se for omitido, stdin será usado.

Restrição— válida apenas no UNIX

Antes de usar pdm_deref no UNIX, a variável de ambiente $NX_ROOT deverá ser definida para o caminho do diretório de instalação do CA SDM e a variável de ambiente PATH deverá incluir $NX_ROOT/bin.

Exemplo: usando pdm_deref para definir os dados para a entrada

Esse exemplo mostra como é possível usar o pdm_deref para configurar os dados para entrada.

Havendo os seguintes dados na tabela ca_location:

```
id    location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB    "Boulder NCC"
```

a seguinte instrução no specfile:

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

alteraria a seguinte entrada:

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

à seguinte saída, que pode ser carregada na tabela ca.contact com pdm_userload:

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

Exemplo: usando pdm_deref para definir os dados para a saída

Esse exemplo mostra como é possível usar o pdm_deref para configurar os dados para saída.

Forneça os seguintes dados na tabela ca_contact:

```
id  last_name first_name
"69499D5A2424884887E62EC9823F5E47"    "Potts"    "Elmore"
```

a seguinte instrução no specfile:

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

alteraria a seguinte entrada:

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

para a saída a seguir, que pode ser impressa ou enviada para uma planilha:

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

Mais informações:

pdm_extract--Extrair dados do banco de dados (na página 1162)

pdm_discimp -- Importação de ativos descobertos

Registro de lote de ativos descobertos que não são do CA SDM. Use isso para pesquisar o MDB em busca de ativos que foram registrados por outros produtos de software e para registrá-los como ativos do CA SDM, para que possam ser usados no CA SDM.

A lógica é semelhante à caixa de diálogo Ativos descobertos que pode ser iniciada a partir do formulário da Web Pesquisa/Lista de ativos. É um processo em lote e interativo.

Esse programa consulta as tabelas ca_logical_asset, ca_asset e ca_logical_asset_property, usando vários parâmetros, e tenta registrar novos Ativos do CA SDM a partir dos valores descobertos.

Sintaxe

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name]
[-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

Critérios de seleção de ativos (use % para caractere curinga):

h

Corresponde a esse rótulo do ativo.

s

Corresponde a esse número de série.

t

Corresponde a esse sinalizador de ativo.

s

Corresponde a esse nome do host.

Critérios de seleção de propriedades de ativos (use % para o caractere curinga):

d

Corresponde a esse nome dns.

M

Corresponde a esse endereço de mac.

Outras opções:

c

A classe do ativo a ser atribuída ao registrar novos ativos proprietários assume como padrão o Hardware descoberto.

A

Modo verboso/diagnóstico.

V

Registrar os ativos, caso contrário, executar no modo de simulação.

h

Exibe essas informações.

o

Gerenciador de objetos (domsrvr) a ser usado para processamento.

Observação: se o processamento resultar em um Rótulo do ativo em branco, o valor encontrado para o nome de host ou Nome de DNS será usado como o Rótulo do ativo. Os ativos devem ter ao menos um Rótulo e Classe do ativo a serem registrados para uso no CA SDM.

Devido à estrutura do MDB e às limitações da arquitetura do CA SDM, duas consultas são executadas para selecionar os registros apropriados. É importante entender isso uma vez que poderia afetar o desempenho. A primeira consulta recupera as linhas de uma junção entre as tabelas ca_logical_asset e ca_asset que combinam rótulo, número de série, marca e nome do host. Então para cada fila resultante, uma consulta é executada em ca_logical_asset_property para encontrar correspondentes a dns_name e mac_address. O ativo da primeira consulta é escolhido para registro se a segunda consulta resulta em retorno de linhas.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira "pdm_task pdm_clean_attachments...".

pdm_discupd -- Atualização do ativo descoberto

Atualização de lote de ativos descobertos que não são do CA SDM. Use esse utilitário para atualizar os ativos que foram importados pelo comando pdm_discimp.

Sintaxe

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

Em que:

t

Teste

A

Modo verboso/diagnóstico.

d

Gerenciador de objetos (domsrvr) a ser usado para processamento.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_edit--Configurar processos do servidor

pdm_edit é usado para editar o arquivo de modelo de inicialização, pdm_startup.tpl, no servidor do CA SDM. Alguns exemplos de quando você necessita editar o arquivo de modelo de inicialização são definir os alias de mecanismo de objeto para configurar o mecanismo da Web para ser executado em um servidor secundário e estabelecer a autenticação remota em um servidor secundário.

Para UNIX

Os usuários UNIX devem alterar as permissões no arquivo pdm_edit.pl para "executável".

Sintaxe

Na instalação de servidor do CA SDM, passe ao diretório $NX_ROOT/samples/pdmconf (UNIX) ou *diretório de instalação*\samples\pdmconf (Windows) e digite o seguinte comando para iniciar o pdm_edit:

```
pdm_perl pdm_edit.pl
```

Observação: pdm_edit é um script Perl e recomenda-se o uso da versão de Perl que vem com o CA SDM, pdm_perl, para executá-lo. Contudo, outras versões de Perl também podem funcionar.

Uso:

Assim que o pdm_edit for executado, será solicitada a inserção de determinadas informações e o restante do processo será conduzido por menus. Para obter informações sobre uso, use a opção de menu H para ajuda. Você também pode exibir a ajuda no arquivo pdm_edit.README usando qualquer editor de texto.

Saída

Quando você sai do pdm_edit e salva suas mudanças, vários arquivos são criados:

- pdm_startup.rmt armazena seus novos valores de configuração
- alias_install.sh (UNIX) ou alias_install.bat (Windows) se você definiu alias de Mecanismo de objeto
- pdm_startup.dat armazena dados que serão necessários na próxima vez que você invocar pdm_edit--mantenha esse arquivo no diretório de trabalho com pdm_edit.pl

Para colocar suas mudanças em vigor, siga essas etapas:

1. Crie um backup do pdm_startup.tpl que reside no diretório $NX_ROOT/pdmconf (Unix) ou *diretório de instalação*\pdmconf (Windows) da instalação do servidor primário CA SDM; em seguida, use o arquivo recém-criado pdm_startup.rmt para substituí-lo.

   Observação: o arquivo pdm_startup.tpl criado a partir de pdm_startup.rmt deve ser legível ao usuário privilegiado

2. Se você definiu os alias de Mecanismo de objeto, execute o script alias_install para reconfigurar seu servidor primário.
3. Execute o utilitário de configuração no servidor primário do CA SDM sem fazer quaisquer mudanças. As novas definições de configuração estarão vigentes na próxima vez que você iniciar o servidor do CA SDM.
4. Caso seja necessário, inicie todos os servidores CA SDM secundários e inicie o servidor principal.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

Mais informações:

Iniciar o servidor primário (na página 58)
Iniciar um servidor secundário (na página 57)

pdm_extract--Extrair dados do banco de dados

O comando pdm_extract extrai dados de tabelas específicas do banco de dados do CA SDM ou o banco de dados inteiro do CA SDM e emite-o como texto no formato ASCII.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] --B] [-f formatstring| ALL | table1
. . . TableN]
```

-c

Produz uma saída de valores separados por vírgula (CSV), tal como:

```
"field1","field2","field3"
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-e

Produz saída CSV (comma-separated value, valor separado por vírgulas) com aspas duplas atuando como seqüência de Escape para aspas duplas incorporadas. Por exemplo:

```
"Texto com uma "seqüência entre aspas""
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-r

Produz saída justificada à esquerda nos formatos se os rótulos de coluna não forem fornecidas no arquivo de entrada:

```
"label":"value"
```

ou

```
"value"
```

Esta opção visa ser usada com impressoras de linhas, por exemplo:

```
Field_Name: Valor do campo
```

As opções de formato de saída -c, -e, -r são mutuamente exclusivas.

-d

Use o formato de data encontrado no arquivo $NX_ROOT/fig/english/cfg/dataent.fmt (UNIX) ou *diretório de instalação*\fig\english\cfg\dataent. fmt (Windows), que você pode editar para adequar às suas exigências.

-h

Exibe informações de ajuda e uso.

-u

Produz saída sem cabeçalhos.

-v

Especifica modo verboso, que escreve comentários sobre o andamento de comando a stdout.

-C

Altera a codificação de UTF-8 para outro conjunto de caracteres. A saída padrão é UTF-8.

Exemplo: para converter a saída para JIS, você executaria "-C iso-2022-jp"

Exemplo: para codificar para o conjunto de caracteres nativo do sistema operacional, use "DEFAULT" ou "NATIVE".

-B

Suprime a marca da requisição de byte se a variável NX_ADD_UTF8_BYTE_ORDER_MARK for definida.

A opção NX_ADD_UTF8_BYTE_ORDER_MARK é uma assinatura em um arquivo. Permite que os editores que oferecem suporte a UTF-8 mantenham a integridade do UTF-8 do arquivo.

Observação: isso é necessário apenas para dados não ASCII. Se não estiver instalado, o comportamento padrão omite a BOM (Byte Order Mark - Marca de Requisição de Byte). Se instalado, defina-o como "1" ou "Sim".

-f *formatstring*

Extrai registros específicos e campos de acordo com *seqüência de formato*, que é uma instrução SQL de subconjunto SQL.

Para uma data depois de um período, use a sintaxe a seguir:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2005-02-24'" > daterange1.txt

Para um intervalo de datas, use a sintaxe a seguir:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2004-01-20' and open_date < DATE '2004-02-25'" > daterange2.txt

Observação: use aspas simples ao redor da data no formato AAAA-MM-DD.

A sintaxe para o comando DATE é:

```
DATE 'aaaa-mm-dd'
```

aaaa = número inteiro representando o ano (entre 1970 e 2038)

mm = número inteiro representando o mês

dd = número inteiro representando o dia

Exemplos:

```
DATE '2005-01-18'
DATE '1999-12-25'
```

A sintaxe para TIMESTAMP é:

```
TIMESTAMP 'aaaa-mm-dd hh.mm.ss[.nnnnnn][[+|-][hh.mm]]
```

aaaa = número inteiro representando o ano (entre 1970 e 2038)

mm = número inteiro representando o mês

dd = número inteiro representando o dia

hh = número inteiro representando a hora

mm = número inteiro representando os minutos

ss = número inteiro representando os segundos

nnnn = número inteiro opcional representando as frações de segundos.

[+|-][hh.mm] = intervalo opcional de fuso horário.

Exemplos:

```
TIMESTAMP '1998-04-28 12:00:00.000000'
TIMESTAMP '2004-10-17 18:30:45'
TIMESTAMP '2005-03-21 12:00:12+08:00'
TIMESTAMP '1999-05-10 09:12:23,005-03:30'
```

Observação a opção -d não é necessária, pois ela afeta apenas o formato da saída.

A seguir é apresentado um exemplo de uso de comando:

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12
12:00:00'"
```

Nesse exemplo, todas as colunas estão sendo extraídas da tabela Call_Req na qual open_date é após a meia-noite de 1/12/2004.

ALL

Extrai a saída de todas as tabelas no banco de dados.

`table1. . . tableN`

Extrai a saída das tabelas especificadas. Os nomes das tabelas devem ser separados por espaços.

O formato padrão, se nenhum for especificado, é um arquivo ASCII compatível com pdm_userload.

Mais informações:

pdm_deref--Retirar referência dos dados ASCII (na página 1154)
pdm_replace--Substituir uma tabela do banco de dados (na página 1184)
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)
rpt_srv--Generate Reports (na página 1204)

pdm_halt--Terminar daemons ou parar serviços

pdm_halt termina completamente todos os daemons do CA SDM (UNIX) ou o Serviço do servidor do sistema (Windows) no sistema a partir do qual pdm_halt é executado. O utilitário pdm_halt normalmente leva aproximadamente 30 segundos para ser concluído. Se demorar mais de dois minutos, pressione Ctrl+C para parar o pdm_halt e, em seguida, tente novamente.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_halt [-w] [-a] [time]
```

-w

Aguarda os daemons pararem.

Uma

Interrompe todos os proctors definidos no arquivo pdm_startup.

[time]

Especifica o número de segundos para aguardar até que o comando seja executado.

Restrições

pdm_halt pode ser executado em um servidor do CA SDM ou em um cliente UNIX do CA SDM. Você deve ser um usuário privilegiado para executar pdm_halt.

pdm_init--Iniciar daemons

Se aplica ao Unix somente

pdm_init inicia todos os processos automáticos do CA SDM a partir do qual o pdm_init é executado. Esses processos automáticos são chamados *daemons* e são executados continuamente na plano de fundo enquanto você trabalha. Nem todos os daemons são iniciados; alguns são aplicáveis apenas a determinados sistemas operacionais. Consulte o capítulo "Gerenciando Servidores" para obter uma lista dos daemons que esse comando pode iniciar.

Observação: use pdm_d_refresh para iniciar os daemons que não falharam ao iniciar na primeira vez depois de solucionar o problema que fez com que eles não iniciassem no primeiro momento. Na maioria dos casos, você não precisa terminar os daemons que estão em execução para iniciar aqueles que falharam inicialmente.

Sintaxe

```
pdm_init
```

Restrições

pdm_init pode ser executado em um servidor do CA SDM ou em um cliente UNIX do CA SDM. Você deve ser um usuário privilegiado para executar pdm_init.

pdm_key_refresh--Atualizar informações-chave armazenadas em cache

O utilitário pdm_key_refresh atualiza as informações-chave armazenadas em cache a partir da tabela-chave de controle no banco de dados. Se as informações-chave de controle forem atualizadas, esse utilitário poderá ser executado em vez de parar e reinicializar o sistema para forçar que o CA SDM use o novo valor de base keyid.

Importante: A mudança da tabela key control pode causar o corrompimento de dados. Não é recomendado tentar alterar as chaves de controle sem instruções específicas do Suporte técnico da CA.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_key_refresh
```

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_lexutil--Modificar o léxico do CA SDM

O utilitário pdm_lexutil permite modificar os léxicos do Service Desk para adicionar ou excluir palavras do dicionário de verificação ortográfica.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_lexutil -a | -d [-f] [-l] wordlist
```

Uma

Adiciona palavras.

-d

Exclui palavras.

-f

Arquivo ou léxico contendo a lista de palavras a serem adicionadas ou excluídas

-l

Nome do léxico.

Padrão: userdict.tlx

wordlist

Palavras a serem adicionadas ou excluídas.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_k_reindex — Utilitário de reindexação de documentos de conhecimento

O utilitário Knowledge Re-Index, pdm_k_reindex.exe, está localizado sob o diretório de instalação do Gerenciamento de conhecimento.

Observação: a reindexação de documentos na base de conhecimento pode ser uma operação que exige tempo, dependendo do tamanho de seu banco de dados. Recomendamos que você execute o utilitário de reindexação de documentos de conhecimento depois de adicionar todas as mudanças.

Para executar a Reindexação de documentos de conhecimento, digite o seguinte comando no prompt de comando:

```
pdm_k_reindex
```

A seguir, as opções disponíveis com esse comando.

Interface:

-d

Define o modo de depuração, como impressão na janela de comando.

-v

Define o modo verboso, como impressão no arquivo stdlog.

-i

Não cria índices de tabela na tabela re-index depois da reindexação.

Observação: os parâmetros com traço, como um prefixo como "–D", devem preceder outros parâmetros que não possuem esse prefixo.

***file*:reindex.txt**

Os documentos são reindexados para o arquivo apropriado.

+i

Cria índices apenas da tabela de reindexação, que será a tabela de pesquisa após a reindexação. Índices antigos serão eliminados antes da reindexação.

+t

Alternar nomes das tabelas search e re-index apenas.

Observação: um prefixo "+" indica que apenas esse parâmetro de aplica.

sdtout

Define a frequência das estatísticas aparecendo na janela de comando. Por padrão, o Utilitário de reindexação de documentos de conhecimento fornece estatísticas na janela de controle a cada 1.000 documentos processados. No entanto, às vezes as estatísticas são exigidas para serem fornecidas com mais frequência. Use o seguinte parâmetro:

```
pdm_k_reindex -i sdtout:10
```

Nesse caso, as estatísticas serão exibidas na janela de comando para cada 10 documentos.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira "pdm_task pdm_clean_attachments...".

Quando usar pdm_k_reindex

Execute o utilitário pdm_k_reindex quando uma ou mais das seguintes configurações de pesquisa tiverem sido alteradas:

- Palavras não pesquisáveis
- Sinônimos
- Termos especiais
- Idioma
- Remover palavras similares
- Remover palavras não pesquisáveis
- Intervalo válido de caracteres
- Reconhecer termos especiais

Uma mensagem apropriada é exibida no nó de Conhecimento da guia Administração quando ocorre uma mudança.

Rastreamento da indexação

Enquanto a reindexação está sendo executada, você pode visualizar o status do processo na seção Rastreamento da indexação na metade inferior da página. Cada campo é descrito da seguinte forma:

Número do documento

Especifica o número de documentos já processados.

Tamanho médio (palavras)

Especifica o tamanho dos documentos atuais, calculado pelo número de palavras menos o número de palavras não pesquisáveis.

Velocidade (docs/seg)

Especifica o número de documentos processados por segundo.

Tempo decorrido

Indica a duração do processo de reindexação desde o início.

Tempo restante

Especifica a quantia de tempo estimada restante para o processo, com base na taxa atual e o número de documentos restante.

No. de falhas

Representa o número de documentos com falha (máximo = 100). Quando o número máximo de falhas é atingido, o administrador é solicitado a continuar com o processo ou cancelar.

Observação: se foram feitas mudanças nas Palavras não pesquisáveis, nos Termos especiais, nos Sinônimos ou nas Configurações de análise e a reindexação não for feita, ela será solicitada na próxima vez quem que o nó Conhecimento na guia Administração for acessado. As mudanças entrarão em vigor somente depois de o Utilitário de reindexação de documentos de conhecimento ser executado.

Importar e reindexar

Quando pdm_kit.exe é invocado a partir da linha de controle, o utilitário pdm_kit importa os documentos no banco de dados. Após o pdm_kit ser concluído, considerando que a indexação ou reindexação do documento não foi desativada usando as opções da linha de comando, o utilitário de reindexação (pdm_k_reindex.exe) é invocado automaticamente. O status e a saída da operação de reindexação são gravados automaticamente em "EBR_REINDEX.LOG" no diretório $NX_ROOT\log.

Configurações de fila de indexação e desindexação para processamento em lote e instantâneo

Tanto a indexação quanto a desindexação executam um processo de lote para incluir um número predefinido de documentos de uma vez. Esses processos de lote são usados para otimização do desempenho. Caso mais documentos sejam incluídos no lote, o desempenho do sistema aumenta.

O número de documentos que podem ser processados é limitado. O limite depende do tamanho dos documentos e dos anexos vinculados. O tamanho do documento é calculado com base no texto puro e seus anexos. Os elementos de formato e imagem não são calculados.

Observação: é possível limitar o tamanho dos anexos ao navegar na Biblioteca de anexos, Repositórios na guia Administração e editar o repositório para definir o Tamanho limite de arquivo (KB).

O tamanho máximo recomendado para o lote é entre 2 e 12 MB (pelo parâmetro EBR_MAX_INDEX_BATCH_SIZE do arquivo NX.env e o tamanho médio de documento).

- Se o tamanho médio de seu documento (incluindo os anexos) for de aproximadamente 0,1 MB, mantenha a configuração padrão no NX.env:

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=128
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=1
  @NX_EBR_INDEX_QUEUE_ONLINE=Yes
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
  ```

  Essa configuração indica que um lote processa 128 documentos, que as execuções de lote têm intervalos de 10 segundos e que ao reindexar, o intervalo de espera entre dos lotes é de 1 segundo.

- Se o tamanho médio de seu documento (incluindo os anexos) for de aproximadamente 0,5 MB, mantenha a configuração padrão no NX.env

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=25
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=10
  @NX_EBR_INDEX_QUEUE_ONLINE=No
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
  ```

  Essa configuração indica que um lote processa 25 documentos, que as execuções de lote têm intervalos de 10 segundos e que ao reindexar, o intervalo de espera entre dos lotes é de 10 segundos.

pdm_listconn--Listar conexões ativas

O utilitário pdm_listconn pode ser usado para listar as conexões ativas para clientes e servidores.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_listconn [-c] [-s] [–s -c] [–t nn] [proc1 [proc2...]]
```

O comando padrão possui o seguinte formato caso nenhum parâmetro seja especificado:

```
pdm_listconn -s -t 2
```

-c

Lista as conexões por cliente. O utilitário exibe duas linhas para cada cliente:

(*n* secs) *tipo_de_cliente nó*|*cproc*

connected to *alias* (*sproc*) at *horas*

n é o número de segundos que o cliente levou para responder.

tipo_de_cliente é "vbop", "animator daemon" ou "web engine".

nó é o endereço IP do nó do cliente.

cproc é o nome do processo slump do cliente.

alias é o alias do servidor com o qual o cliente está conectado.

sproc é o nome do processo slump do servidor.

horas é o horário da conexão.

Por exemplo:

```
(0 secs) vbop client 141.202.211.34|vbop-0x40120000:anthill:0
        connected to CMD40120 on anthill (domsrvr) at 19/02/99 10:44:16
```

-s

Lista as conexões por servidor (padrão). O utilitário exibe duas linhas para cada servidor:

(*n* seg) servidor *alias* (*nó*|*sproc*) aceitação *aceitação*
contar clientes conectados (use pdm_listconn -c -s para listar os clientes por servidor)

n é o número de segundos que o servidor levou para responder.

nó é o endereço IP do nó do servidor.

alias é o alias do servidor com o qual o cliente está conectado.

sproc é o nome do processo slump do servidor.

aceitação é a aceitação de novos clientes por parte do (0 - 100).

contagem é o número de clientes conectados.

Por exemplo:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 clientes conectados (use pdm_listconn -c -s para listar os clientes por servidor)
   vbop client 141.202.211.34|vbop2 connected 19/02/99 10:53:16
   vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 19/02/99
10:44:17
```

-s -c

Lista as conexões por servidor, incluindo detalhes do cliente para cada servidor. O utilitário exibe várias linhas para cada servidor:

(*n* seg) servidor *alias* (*nó*|*sproc*) aceitação *aceitação*
contar clientes conectados:
client_type node|cproc connected time

onde:

n é o número de segundos que o servidor levou para responder.

nó é o endereço IP do nó do servidor.

alias é o alias do servidor com o qual o cliente está conectado.

sproc é o nome do processo slump do servidor.

aceitação é a aceitação de novos clientes por parte do (0 - 100).

contagem é o número de clientes conectados.

tipo_de_cliente é "vbop", "animator daemon" ou "web engine".

nó é o endereço IP do nó do cliente.

cproc é o nome do processo slump do cliente.

horas é o horário da conexão.

Por exemplo:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
dois clientes conectados:
    vbop client 141.202.211.34|vbop2 connected 19/02/99 10:53:16
    vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 19/02/99
10:44:17
```

-t nn

Especifica um intervalo de tempo limite em segundos. Pelo fato de o pdm_listconn receber informações de um número desconhecido de clientes e servidores, ele é encerrado quando o intervalo de tempo de inatividade termina após a última mensagem ser recebida.

Padrão: 2

proc1

Especifica um ou mais procnames de slump, separados por espaços. O utilitário exibe as informações sobre cliente ou servidor deles, conforme apropriado.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_load--Adicionar, atualizar e excluir registros do banco de dados

Importante: Usar o pdm_load pode ser destrutivo, portanto, sempre faça backup de seu banco de dados antes de executar um pdm_load e use pdm_userload, a não ser que instruído a usar o pdm_load.

O pdm_load atualiza um banco de dados do CA SDM usando um arquivo de entrada que você especifica, com no máximo 112 atributos.

Sempre que você carrega os tickets (como solicitações ou ocorrências), seu número de ticket deve incluir um prefixo ou sufixo exclusivo em sua seqüência. O CA SDM vê este número como uma seqüência de caracteres, não como um número seqüencial, e assim não pode garantir que atribuirá um número exclusivo aos tickets carregados. Assim que você atribuir um prefixo ou sufixo exclusivo usando awk ou outro processador de texto, poderá carregar tickets sem que o CA SDM grave sobre os números atribuídos anteriormente.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v] –f filename
```

As entradas de arquivo de entrada seguem este formato:

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name é o nome da tabela a ser carregada, conforme listado no arquivo de esquema do banco de dados do CA SDM, localizado em $NX_ROOT/site/schema.sch (UNIX) ou *diretório de instalação*\site\schema.sch (Windows). $NX_ROOT ou *diretório de instalação* é o diretório em que oCA SDM foi instalado.

-f *filename*

Especifica um arquivo ASCII de entrada.

-c

Compara o arquivo de entrada com o banco de dados e informa as atualizações que devem ser feitas, mas não faz as atualizações.

-m

Especifica atualização em massa. Especifique quando estiver usando pdm_load para adicionar ou excluir um grande número de registros. Essa opção suprime todas as notificações do cliente de atualizações e envia uma mensagem de atualização no cache para uma tabela quando pdm_load concluir o processamento da tabela.

-r

Remove registros de banco de dados que correspondam a registros de entrada.

Importante: Faça uma cópia de backup do banco de dados antes de executar o pdm_load com essa opção. Uma vez removidos os registros antigos do banco de dados, você deverá restaurar o banco de dados do CA SDM com esta cópia de backup se desejar recuperar quaisquer registros excluídos.

-u

Atualiza registros existentes, mas não insere novos registros no banco de dados.

Mais informações:

pdm_backup--Gravar banco de dados no arquivo ASCII (na página 1149)
pdm_replace--Substituir uma tabela do banco de dados (na página 1184)
pdm_restore--Restaurar um banco de dados (na página 1187)
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)

pdm_logfile--Alterar o tamanho de cutover de stdlog

pdm_logfile permite alterar o tamanho de cutover de stdlog.*x*. O cutover pode ocorrer depois da gravação de um número especificado de bytes. Em UNIX, esse valor é redefinido com cada pdm_init. No Windows, as configurações são mantidas com cada pdm_halt e pdm_init.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_logfile [-L|-h]
```

ou

```
pdm_logfile [-g -h] [-b bytes]
```

Exemplo:

Para alterar seus arquivos stdlog.*x* para cutover em 500.000 bytes, emita o seguinte comando:

```
pdm_logfile -f STD -b 500000
```

-L

Cria uma lista de cutovers atuais.

-q

Executa pdm_logfile em modo silencioso.

-b bytes

Especifica o número de bytes gravados antes de ocorrer o cutover.

Restrições

Você pode executar o pdm_load enquanto o CA SDM estiver ativo, mas o desempenho pode se tornar muito lento. É melhor executar o pdm_load quando ninguém está usando o CA SDM.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

pdm_log4j_config Utility--Modify the log4j properties File

O utilitário pdm_log4j_config.pl permite configurar o arquivo de propriedades log4j do CA SDM, os componentes web, o PDM_RPC, a Automação de suporte, o Rest e o CMDB Visualizer. Execute o scrip do lote do utilitário com base no ambiente. Para Windows, execute o pdm_log4j_config a partir da linha de comando. Para Unix, execute o arquivo pdm_log4j _config.sh.

Esse comando apresenta o seguinte formato:

```
pdm_log4j_config –f <component> -d
pdm_log4j_config -h
pdm_log4j_config –f <component> [-a | -n <name>] [-l <log level>] [I <max # of log files>] [-s <max size of log files>] [-t <log level threshold>]
```

-f

Especifica a configuração do log4j do CA SDM ou o componente do CA SDM que você deseja alterar. Use um dos seguintes valores:

SDM_WEB, SDM_RPC, REST, SA ou Viz.

Observação: use a opção obrigatória juntamente com outras opções.

-d

Exibe a configuração atual do log4j.properties.

-h

Exibe ajuda para o utilitário.

Uma

Conclui todas as mudanças ao log4j.properties, globalmente.

-n

Especifica se você deseja modificar uma classe específica ou nome do pacote.

Especifique um nome de classe específico, como bop_logging ou de um pacote completo, como com.ca.ServicePlus.

-l

Especifica o nível de log que você deseja definir.

Observação: especifique a opção -a ou -n.

-i

Especifica o índice de número máximo de arquivos que você deseja definir.

Observação: especifique a opção -a ou -n.

-s

Especifica o tamanho máximo do arquivo que você deseja definir.

Observação: especifique a opção -a ou -n.

Importante: Altere o appender no arquivo log4j.properties do Visualizer para Appender de arquivo contínuo, antes de executar o comando com esse parâmetro. Se você não alterar o appender, o MaxFileSize gera logs no mesmo arquivo.

-t

Especifica o limite do nível de log .

Observação: especifique a opção -a ou -n.

Exemplos de uso do utilitário

A lista a seguir mostra exemplos de uso do utilitário pdm_log4j_config:

- Modificar o nível de verbosidade de todos os agentes de log configurados no arquivo de propriedades usando as variáveis -l e -a .

  Por exemplo, defina todos os agentes de log configurados no Support Automation para um nível de DEPURAÇÃO:

  ```
  pdm_log4j_config –f SA -a -l DEBUG
  ```

- Modificar o nível de verbosidade de uma classe de agente de log específica ou nome do pacote no arquivo de propriedades log4j do CA SDM usando as variáveis -l e -n.

  Por exemplo, defina o agente de log para o pacote pdm_rpc para DEBUG usando um dos seguintes exemplos de código:

  ```
  pdm_log4j_config –f SDM_RPC -n pdm_rpc -l DEBUG
  ```

  ```
  pdm_log4j_config –f SDM_RPC -n com.ca.ServicePlus.pdm_rpc -l DEBUG
  ```

- Modifique o número máximo de arquivos de log para criar para todos os appenders (propriedade MaxBackupIndex) usando as variáveis -i e -a no arquivo de propriedades log4j do REST.

  Por exemplo, defina o número máximo de arquivos para todos os appenders para 9.

  ```
  pdm_log4j_config –f REST -a -i 9
  ```

- Modificar o número máximo de arquivos de log configurados no arquivo de propriedades log4j do CA SDM para criar um appender de uma classe específica ou de um conjunto de classes (propriedade MaxBackupIndex) usando as variáveis -i e -n.

  Por exemplo, defina o número máximo de arquivos para bop_logging para 7.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -i 7
  ```

- Modificar o tamanho máximo de cada arquivo de log configurado no arquivo de propriedades log4j do REST para criar qualquer appender (propriedade MaxFileSize) por meio das variáveis -s e -a.

  Por exemplo, defina o número máximo de arquivos para todos os appenders para 9 MB.

  ```
  pdm_log4j_config –f REST -a -s 9MB
  ```

- Modificar o número máximo de arquivos de log configurados no arquivo de propriedades log4j do CA SDM para criar um appender de uma classe específica ou de um conjunto de classes (propriedade MaxFileSize) usando as variáveis -s e -n.

  Por exemplo, defina o número máximo de arquivos para bop_logging para 7 MB.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -s 7MB
  ```

- Modificar o limite do nível de log de todos os appenders configurados no arquivo de propriedades log4j da Automação de Suporte (propriedade do Limite), usando as variáveis -t e -a.

  Por exemplo, defina o limite do nível de log como DEBUG.

  ```
  pdm_log4j_config –f SA -a -t DEBUG
  ```

  Observação: o limite do nível de log para o parâmetro -t substitui o nível de log para o parâmetro -l. Se você modificar o nível de log e o nível de limite, os logs de depuração do servlet não aparecem no arquivo.

- Modificar o limite do nível de log de um appender de uma classe específica ou um conjunto de classes (Limite propriedade) configurados no arquivo de propriedades log4j do CA SDM usando as variáveis-t e -n.

  Por exemplo, defina o limite do nível de log como WARN.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -t WARN
  ```

- Execute o comando a seguir para exibir a configuração atual do agente de log e appender do arquivo de propriedades log4j do REST:

  ```
  pdm_log4j_config –f REST -d
  ```

Importante: Usar as variáveis -l, -i e -t juntamente com uma das opções -a ou -n; não usar ambas as opções. A opção -f é obrigatória. As opções -h e -d são mutuamente exclusivas para qualquer outra opção.

Modificar o intervalo de atualização do arquivo de log manualmente

Os administradores podem modificar a frequência com que o CA SDM monitora as mudanças ao arquivo log4j.properties. Por padrão, o intervalo de atualização é definido para 60 segundos. Os componentes do CA SDM, incluindo Servlets do SDM, PDM_RPC, Support Automation, CMDB Visualizer e REST usam o log4j para registro.

Siga estas etapas:

1. Abra o diretório a seguir no servidor do CA SDM:

   `NX_ROOT`

2. Abra o arquivo NX.env para edição.
3. Modifique a variável NX_LOG4J_REFRESH_INTERVAL com um valor em milissegundos.

   Observação: se você inserir um valor negativo ou não numérico, o valor padrão é de 60 segundos.

4. Salve o arquivo NX.env.

Modificar o appender o jsrvr.log

Por padrão, os servlets como PDMContextListener, pdmweb, UploadServlet e pdm_report registram mensagens de nível de INFO no arquivo jsrvr.log. É possível alterar o nível de limite do appender jsrvr.log para registrar quaisquer mensagens no nível INFO.

Siga estas etapas:

1. Modifique o nível no arquivo log4j.properties para o limite a seguir:

```
log4j.appender.jsrvrlog.Threshold=debug
```

2. Modifique o nível de log de UploadServlet:

```
log4j.logger.com.ca.ServicePlus.uploadservlet=debug, jsrvrlog
```

3. Abra o arquivo jsrvr.log.
4. Confirme que as mensagens de log de depuração de UploadServlet são exibidas.

Observação: se você modificar o nível de log sem modificar o nível de limite, os logs de depuração do servlet não aparecem no arquivo. Nem todos os servlets possuem loggers explícitos vinculados. Por exemplo, o arquivo log4j.properties, não inclui pdmweb, BOServlet, pdm_export, pdm_report e pdm_cache, que são parte do pdmweb servlet. Para consultar os logs de depuração desses servlets, modifique o nível de log pdmweb.

Modificar o appender o jstd.log

Todos os logs de aplicativos nonwebapp despejam separadamente no arquivo jstd.log. É possível exibir os logs de um desses aplicativos, como pdm_rpc, alterando o nível de log daquele aplicativo específico.

Siga estas etapas:

1. Modifique o nível de log a seguir:

```
log4j.logger.com.ca.ServicePlus.pdm_rpc=debug
```

2. Abra log4j.properties e confirme se as entradas do log são exibidas.

pdm_proctor_init--Iniciar solicitador em servidores secundários

Se aplica ao Unix somente

Use o pdm_proctor_init para iniciar o solicitador em servidores secundários. Todos os servidores secundários devem ser iniciados antes de iniciar os daemons do servidor primário. Depois que todos os daemons tiverem sido parados no servidor primário, use pdm_halt no servidor secundário para parar esse solicitador.

Observação: não use pdm_proctor_init no servidor principal.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_proctor_init
```

pdm_replace--Substituir uma tabela do banco de dados

pdm_replace exclui uma tabela em um banco de dados do CA SDM e a substitui por uma tabela de um arquivo temporário que você especifica com a opção -f; os dados do arquivo de entrada são os únicos que estarão nessa tabela depois da execução de pdm_replace. Faça backup de sua tabela antes de executar pdm_replace.

Observação: como parte de seu processamento, o pdm_replace primeiro encerra os daemons (UNIX) ou os serviços (Windows).

pdm_replace aceita um arquivo de texto como entrada, que é o mesmo formato de arquivo usado por pdm_userload. É possível criar um arquivo de entrada para pdm_replace usando pdm_extract; no entanto, você não pode usar a saída de pdm_backup como entrada para pdm_replace.

Importante: Certifique-se de nomear seu arquivo de entrada com um nome diferente do nome da tabela que você está tentando substituir. Por exemplo, se você estiver substituindo uma tabela chamada ca_contacts e denominar o arquivo de entrada como ca_contacts.dat, após a execução do comando pdm_replace para apontar para o arquivo de entrada (ca_contacts.dat), a execução excluirá o arquivo porque ele tem o nome igual ao da tabela.

Restrições

- pdm_replace pode ser executado apenas em um servidor do CA SDM.
- Apenas um usuário privilegiado ou raiz pode executar pdm_replace.
- Não execute pdm_replace quando os usuários estiverem conectados ao CA SDM.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_replace [-v] -f filename
```

-v

Especifica modo verboso.

-f *filename*

Especifica um arquivo ASCII com o seguinte formato:

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

Esse formato é igual ao formato de arquivo usado por pdm_userload. É possível criar um arquivo de entrada para pdm_replace usando pdm_extract; no entanto, você não pode usar a saída de pdm_backup como entrada para pdm_replace.

Mais informações:

pdm_extract--Extrair dados do banco de dados (na página 1162)
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)

pdm_rest_util – Gerenciar o aplicativo serviços web do CA SDM RESTful

O CA SDM usa esse utilitário automaticamente. É possível executá-lo manualmente se você precisar do utilitário, por exemplo, após um erro inesperado. Esse utilitário de serviços web do REST implementa o aplicativo da web para serviços do REST. Esse utilitário instala o aplicativo REST na instância do Tomcat do REST. Um arquivo de lote no diretório NX_ROOT\bin (pdm_rest_util.bat no Windows ou ./pdm_rest_util.sh no UNIX) permite chamar o utilitário.

Este comando tem os seguintes formatos e opções:

```
pdm_rest_util –h | [-deploy] | [-undeploy]
```

-h

Imprime a ajuda da linha de comando.

-deploy

Gera, compila e implanta todas as fábricas Majic.

-undeploy

O REST desinstala os serviços web no servidor local.

Cancela a implantação do aplicativo de serviços web do REST

É possível cancelar a implantação do aplicativo de serviços web do REST com o utilitário pdm_rest_util. Por exemplo, se você quiser executar a manutenção do CA SDM e preferir cancelar a implantação do REST durante essa operação.

Siga estas etapas:

1. Abra um prompt de comando.
2. Execute o seguinte comando:

   ```
   pdm_rest_util -undeploy
   ```

   O aplicativo de serviços web do REST está desinstalado.

Importante: Se você cancelar a implantação do aplicativo REST com esse utilitário, o REST pode reimplantar automaticamente quando o CA SDM for reiniciado. Recomendamos que você use a configuração do CA SDM para desativar o REST indefinidamente.

pdm_restore--Restaurar um banco de dados

pdm_restore pára o CA SDM e, em seguida, exclui todos os registros de um banco de dados do CA SDM e os substitui por registros de um arquivo que você especifica com a opção -f. Os dados do arquivo de entrada são os únicos dados que estarão no banco de dados do CA SDM depois da execução de pdm_restore.

O arquivo de entrada deve ser criado usando pdm_extract ou pdm_backup, ou ser formatado para pdm_restore. pdm_backup pode fazer backup de dados que não são do banco de dados, e pdm_restore pode restaurar esses dados. pdm_backup e pdm_restore não são recomendados quando outras ferramentas de backup e restauração estiverem disponíveis.

Observação: como parte de seu processamento, o pdm_restore primeiro encerra os daemons (UNIX) ou os serviços (Windows).

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_restore [-d] [-g] [-n] [-w] [-v] –f filename
```

Restrições

pdm_restore pode ser executado apenas em um servidor do CA SDM. Apenas um usuário privilegiado ou raiz pode executar pdm_restore.

Importante: Use pdm_restore apenas com um backup completo de banco de dados criado por pdm_backup, já que o banco de dados atual será excluído e substituído pelo arquivo de backup. Não execute pdm_restore quando os usuários estiverem conectados ao CA SDM.

-d

Especifica que apenas os dados do banco de dados serão restaurados.

-g

Especifica que apenas os dados que não são do banco de dados serão restaurados. Apenas as janelas (formulários) e outros dados que não são do banco de dados serão restaurados.

-n

Especifica que NX.env será restaurado se estiver restaurando dados que não são do banco de dados. Por padrão, NX.env não é restaurado. Recomendamos que o arquivo NX.env não seja restaurado, a menos que a restauração seja no mesmo servidor de origem do backup. A restauração de um NX.env incorreto pode afetar os bancos de dados não planejados.

-w

Especifica que web.cfg será restaurado se estiver restaurando dados que não são do banco de dados. Por padrão, web.cfg não é restaurado.

-v

Especifica modo verboso.

-f *filename*

Especifica um arquivo de entrada que contém um backup completo criado por pdm_backup.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

Mais informações:

Restauração do banco de dados (na página 487)
pdm_backup--Gravar banco de dados no arquivo ASCII (na página 1149)
pdm_userload--Adicionar, atualizar e excluir registros do banco de dados (na página 1196)

pdm_status--Mostrar status de daemons ou processos

pdm_status mostra o status de todos os daemons do CA SDM (UNIX) ou processos (Windows) no sistema a partir do qual o comando é executado.

A saída é exibida neste formato:

```
DAEMON                          STATUS      HOST      PID   SLUMP CONNECT TIME
------------------------------------------------------------------------------
Agent anthill                   Running     anthill   455   Tue Feb 17 17:55:12
Ddict_rd              (ddictrd) Completed   anthill
Data Dictionary    (ddictbuild) Completed   anthill
...
User Validation       (boplgin) Running     anthill   456   Tue Feb 17 17:55:21
```

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_status
```

pdm_task--Definir variáveis de ambiente

Se aplica ao Unix somente

O utilitário pdm_task define as variáveis de ambiente para os comandos que não têm invólucros. Por exemplo, o comando pdm_task deve anteceder o comando de relatório na linha de comando **somente** quando o comando é invocado por uma seqüência ou linha de comando. Se você emitir o comando report de um menu, não precisa incluir pdm_task, porque todas as variáveis de ambiente são definidas pelo aplicativo.

Observação: Os relatórios não podem ser gerados a partir da linha de comando em um cliente.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_task comando
```

comando

Especifica um comando que não tem um invólucro e, portanto, não define automaticamente as variáveis de ambiente. Consulte relatório--Gerar relatórios (na página 1203) para obter mais informações sobre como executar o pdm_task com um comando.

pdm_text_cmd--Interface da linha de comando API do texto

Use o comando pdm_text_cmd para a API do texto que você pode usar para criar e atualizar vários objetos tal como solicitações, requisições de mudança, ocorrências, ativos e contatos.

Importante: Não é possível usar aspas simples ou duplas como o parâmetro dos comandos pdm_text_nxd or bop_cmd.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_text_cmd –t table {-u from_userid –p from_persid} [-o operation] [-f input file]
[-T timeout] [-h]
```

tabela *-t*

(Obrigatório) Especifica a tabela a ser processada. O nome da *tabela* pode ser um dos seguintes valores (não diferencia maiúsculas de minúsculas):

- Ativo
- Contato
- Mudança
- Ocorrência
- Solicitação

Observação: consulte a seção [OPTIONS] do arquivo text_api.cfg para obter uma lista completa de nomes de tabela válidos.

-u *from_userid* **| -p** *from_persid*

(Obrigatória uma opção) Identifica o contato para essa operação:

-u *from_userid*

Identifica o contato usando o valor da ID de Usuário.

-p *from_persid*

Identifica o contato usando o identificador de objeto exclusivo para o registro de contato. *from_persid* deve estar na forma **cnt:***xxxx. xxxx* é a ID persistente do objeto.

Observação: o valor que você especifica com essa opção é anexado ao final da entrada para o comando pdm_text_cmd usando a palavra-chave apropriada, %FROM_USERID ou %FROM_PERSID

-o *operation*

Especifica a operação a ser executada. A *operação* deve ser um dos seguintes valores (não faz distinção entre letras maiúsculas e minúsculas):

- NEW — cria um objeto. Este valor é o padrão caso nenhuma operação seja especificada.
- UPDATE | UPD — cria um objeto se não for encontrado ou atualiza um objeto existente caso seja encontrado.
- UPDATE_ONLY | UPDO — atualiza o objeto caso seja encontrado. Caso contrário não realiza nenhuma ação.

Tanto UPDATE quanto UPDATE_ONLY precisam da palavra-chave %SEARCH na entrada do comando. Você pode executar apenas uma transação de operação com cada invocação de pdm_text_cmd.

-f *input_file*

Especifica o completo caminho do arquivo a ser processado, que é um arquivo de texto contendo comandos válidos de API de texto. Caso esse parâmetro seja omitido, os comandos são usados a partir do STDIN. A API de texto usa o seguinte formato básico para entrada:

```
%palavra-chave=valor
```

É possível emitir diversos comandos na entrada ao separar a solicitação de comando por pelo menos cinco sinais de porcentagem (%%%%%).

Observação: para obter mais informações sobre as palavras-chave válidas e sobre a entrada de formatação na API de texto, consulte o arquivo text_api.cfg.

-T *timeout*

Especifica o número de segundos que se deve esperar para uma resposta do servidor antes da expiração. O padrão é 30 segundos.

Observação: pdm_text_cmd mostra as respostas com base em texto recebidas novamente da API de texto, que incluem mensagens de erros ou êxito e o texto original enviado usando a API para processamento. O pdm_text_cmd retorna zero se o comando for concluído com sucesso sem aviso ou erros ou se um comando for concluído com sucesso, mas com avisos. Qualquer outro valor de retorno indica que ocorreu um erro.

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

Observação: ao transmitir os parâmetros no prompt de comando, use Ctrl+Z no Windows e Ctrl+D no POSIX.

(novo grupo relacionado 1)

Usando a API de texto (na página 509)

Exemplos de entrada

O pdm_text_cmd é a interface da linha de comando para a API do texto, que você pode usar para criar e atualizar vários objetos, tal como solicitações, requisições de mudança, ocorrências, ativos e contatos.

Exemplo: Usar um arquivo de entrada para criar uma ocorrência

O exemplo a seguir demonstra como usar um arquivo de entrada pdm_text_cmd para criar uma ocorrência:

```
%DESCRIPTION=This is my Test.
%PRIORITY=3
```

Para processar esse arquivo, considerando que seu caminho completo fosse c:\input.txt, você emitiria o seguinte comando:

```
pdm_text_cmd -t Issue –u user01 -f c:\input.txt
```

Exemplo: Usar um arquivo de entrada para atualizar uma ocorrência

O exemplo a seguir demonstra um arquivo de entrada para atualizar a ocorrência 123 para uma prioridade 2:

```
%SEARCH=ISSUE_ID
%ISSUE_ID=123
%PRIORITY=2
```

Para processar esse arquivo, considerando que seu caminho completo fosse c:\update.txt, você emitiria o seguinte comando:

```
pdm_text_cmd -t Issue -o UPDATE_ONLY –u user01 -f c:\update.txt
```

Exemplo: Usar um arquivo de entrada para criar várias solicitações

O exemplo a seguir demonstra a criação de várias solicitações com um arquivo de entrada. Este comando pode ser útil ao criar dados de teste em um sistema de teste.

```
%DESCRIPTION=This is Test 1.
%PRIORITY=3
%%% % %
%DESCRIPTION=This is Test 2.
%PRIORITY=2
%%% % %
%DESCRIPTION=This is Test 3.
%PRIORITY=None
```

Para processar esse arquivo, considerando que seu caminho completo fosse c:\testdata.txt, você emitiria o seguinte comando:

```
pdm_text_cmd -t Request –u user01-f c:\testdata.txt
```

pdm_uconv--Convert Local Charset to UTF-8

O utilitário pdm_uconv auxilia na conversão de dados de releases anteriores do CA SDM ou integrações com outros produtos CA Technologies. O uso mais comum para esse utilitário é realizar a conversão do conjunto de caracteres local para UTF-8 e de UTF-8 para o conjunto de caracteres local.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -i]
[--fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-signature]
[-o] [file ...]
```

-h

Abre o menu de ajuda.

-V

Imprime a versão do programa.

-s

Usa a operação silenciosa e suprime as mensagens.

-v

Exibe as informações de progresso do utilitário.

-l

Lista todas as codificações disponíveis. As seguintes opções são válidas:

--list-code

Lista apenas a codificação determinada.

--default-code

Lista apenas a codificação padrão.

-L

Lista todas as transliterações disponíveis.

--cannon

Imprime a lista no formato cnvrtrs.txt(5).

-x

Executa o progresso através da transliteração.

--to-callback *callback*

Usa o retorno de chamado na codificação do destino.

-c

Omite caracteres inválidos da saída.

--from-callback *callback*

Usa o retorno de chamado na codificação original.

-i

Ignora sequências inválidas na entrada.

--callback *callback*

Usa o retorno de chamado em ambas as codificações.s.

-b

Especifica o tamanho do bloco.

Padrão: 4096

--fallback

Usa o mapeamento de retorno.

--no-fallback

Não usa o mapeamento de retorno.

-f

Define a codificação original.

-t

Define a codificação de destino.

--add-signature

Adiciona o caractere de assinatura Unicode U+FEFF (BOM).

--remove-signature

Remove o caractere de assinatura Unicode U+FEFF (BOM)

-o

Grava a saída no arquivo.

Exemplos:

A partir do conjunto de caracteres para o UTF-8

pdm_uconv -t utf-8 inputfile.txt > outputfile.txt

A partir do conjunto de caracteres específico (iso-2022-jp) para UTF-8

pdm_uconv -f iso-2022-jp -t utf-8 inputfile.txt > outputfile.txt

A partir do UTF-8 para o conjunto de caracteres local

pdm_uconv -f utf-8 inputfile.txt > outputfile.txt

A partir do UTF-8 para o conjunto de caracteres específico.

```
pdm_uconv -f utf-8 -t iso-2022-jp inputfile.txt > outputfile.txt
```

O utilitário pdm_uconv possui os seguintes retornos de chamado válidos:

- substituir
- skip
- parar
- escape
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_userload--Adicionar, atualizar e excluir registros do banco de dados

O utilitário pdm_userload atualiza um banco de dados do CA SDM usando um arquivo de entrada especificado.

Importante: Você sempre deve fazer backup do banco de dados antes de executar um pdm_userload.

Sempre que você carregar tickets (como ocorrências ou solicitações), seu número de ticket deve incluir um prefixo ou sufixo exclusivo em sua seqüência. O CA SDM vê este número como uma seqüência de caracteres, não como um número seqüencial, e assim não pode garantir que atribuirá um número exclusivo aos tickets carregados. Desde que você atribua um prefixo ou sufixo exclusivo usando awk ou outro processador de texto, entretanto, poderá carregar tickets sem que o CA SDM grave sobre os números atribuídos anteriormente.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m] –f filename
```

Formato de arquivo de entrada

As entradas de arquivo de entrada seguem este formato:

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

nome_da_tabela é o nome da tabela a ser carregada, conforme listado no arquivo de esquema do banco de dados do CA SDM, localizado em $NX_ROOT/site/schema.sch (Unix) ou *diretório de instalação*\site\schema.sch (Windows), onde $NX_ROOT ou *diretório de instalação* é o diretório onde você instalou o CA SDM.

-f filename

Especifica um arquivo ASCII de entrada.

Uma

Atualiza todos os registros existentes, independentemente de mais de um registro existente corresponder a um único registro de entrada. Sem essa opção, os registros de entrada que correspondem a mais de um registro existente são rejeitados.

Importante: Use essa opção com cuidado.

-c

Compara o arquivo de entrada com o banco de dados e informa as atualizações que devem ser feitas, mas não faz as atualizações.

-r

Remove registros de banco de dados que correspondam a registros de entrada. A opção -a pode ser usada com a opção -r.

Observação: faça uma cópia de backup do banco de dados antes de executar pdm_userload com essa opção. Uma vez removidos os registros antigos do banco de dados, você deverá restaurar o banco de dados do CA SDM com esta cópia de backup se deseja recuperar quaisquer registros excluídos.

-v

Especifica modo verboso.

-u

Atualiza registros existentes, mas não insere novos registros no banco de dados.

-m

Significa atualização em massa. Especifique quando estiver usando pdm_userload para adicionar ou excluir um grande número de registros. Essa opção suprime todas as notificações do cliente de atualizações e envia uma mensagem de atualização de cache para uma tabela quando pdm_userload termina o processamento da tabela.

-x

Usa formatos de entrada numérica sensíveis ao local.

-t

Especifica o nome ou UUID do inquilino para associar todos os dados carregados com o inquilino especificado. Esse argumento é válido apenas quando a multilocação está instalada.

O Pdm_userload oferece suporte a novos argumentos na instrução TABLE, "Truncate" e "NoNewID". Esses argumentos são especificados em uma opção facultativa entre parênteses após o nome da tabela. Por exemplo:

```
TABLE Call_Req (TRUNCATE, NONEWID)
```

Truncate

Faz com que o pdm_userload emita um comando TRUNCATE específico do banco de dados para a tabela antes de carregar quaisquer dados. Além disso, ele força a lógica do pdm_userload a usar apenas a lógica de inserção independente dos argumentos da linha de comando, uma vez que todos os registros são novos.

NoNewID

Faz com que o pdm_userload use o valor da id de seu arquivo de controle de entrada para as novas linhas na tabela, em vez de gerar uma nova ID para os dados inseridos (a lógica padrão da opção pdm_userload -i).

Restrições

Você pode executar o pdm_userload enquanto o CA SDM estiver ativo, mas o desempenho pode se tornar muito lento. É melhor executar opdm_userload quando ninguém está usando o CA SDM.

Mais informações:

pdm_backup--Gravar banco de dados no arquivo ASCII (na página 1149)
pdm_replace--Substituir uma tabela do banco de dados (na página 1184)
pdm_restore--Restaurar um banco de dados (na página 1187)

pdm_webstat--Retornar estatísticas de uso da Web

Use pdm_webstat para retornar as estatísticas do usuário e da sessão do CA SDM para um ou mais processos do mecanismo da Web. O comando pdm_webstat mostra as sessões cumulativas, número máximo de sessões em um dado momento e as sessões ativas atuais. Também pode fornecer informações sobre usuários individuais.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p webengine process] [-n] [-h]
```

-r

Especifica o modo de texto bruto, sem títulos ou outra formatação. Na saída para um único processo do mecanismo da Web não há quebras de linha; contudo, a saída para cada processo do mecanismo da Web sempre começa em uma nova linha.

O modo de texto bruto exibe os dados exatamente na mesma requisição de quando você usa pdm_webstat sem a opção -r. Use o modo de texto bruto se quiser usar os dados resultantes em uma planilha ou em outro tipo de relatório. Por exemplo, a sintaxe a seguir:

```
pdm_webstat -r
```

exibe a seguinte saída:

```
10/11/2005 10:31:49 web:local:0 12 4 2
10/11/2005 10:31:49 web:local:1 9 2 2
```

-d

Especifica a saída detalhada que exibe sessões do usuário. A opção -d lista todas as sessões atuais no formato *id_do_usuário@Endereço_IP*. Se uma sessão for exibida sem uma ID de usuário, normalmente significa que não foi efetuado logon na sessão ainda. Por exemplo, a sintaxe a seguir:

```
pdm_webstat -d
```

exibe a seguinte saída:

```
PDM_Webstat: Invoked at 10/11/2005 10:27:31
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16
  usery@192.168.1.20
=========================================
Report from Webengine: web:local:1
=========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14
  userx@192.168.1.8
```

-d

Fornece saída mais detalhada para fins de depuração. Essa opção deve ser especificada apenas quando solicitado especificamente pelo suporte da CA. Ela adiciona informações internas sobre cada sessão na saída detalhada. Por exemplo, a sintaxe a seguir:

```
pdm_webstat -D
```

exibe a seguinte saída:

```
PDM_Webstat: Invoked at 10/11/2007 10:28:10
==========================================
Report from Webengine: web:local:0
==========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16           SessionStat   1
  userx@192.168.1.20      SessionStat   5
==========================================
Report from Webengine: web:local:1
==========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14   SessionStat   7
  userx@192.168.1.8       SessionStat  13
```

-i

Especifica um intervalo em segundos entre relatórios sucessivos. Quando o argumento -i é especificado, pdm_webstat é executado continuamente. O comando pdm_webstat envia a saída de seu relatório no formato solicitado por outros argumentos, aguarda pelo intervalo especificado e envia a saída do relatório novamente. Com –i, o pdm_webstat termina apenas quando cancelado explicitamente, normalmente com Ctrl+C. Por exemplo, a sintaxe a seguir:

```
pdm_webstat –i 5 –p web:local –r
```

exibe a seguinte saída:

```
09/21/2007 16:27:25 web:local 14 10 6
09/21/2007 16:27:30 web:local 17 10 9
09/21/2007 16:27:35 web:local 18 10 10
09/21/2007 16:27:41 web:local 21 13 13
```

-t timeout

Especifica um valor de tempo limite em segundos. Esse parâmetro faz com que o pdm_webstat espere por um número de segundos para obter uma resposta antes de terminar. O padrão é 30 segundos.

-p webengine_process

Especifica o nome do processo do mecanismo da Web para o qual você deseja emitir o relatório. Por padrão, para todos os processos do mecanismo da Web são emitidos relatórios. O nome do processo (também chamado de nome do slump) é o mesmo nome que seria exibido em uma saída de slstat e sempre começa com "web:".

-n

Especifica a entrada de log normal para cada mecanismo da web relatado. Por padrão, é criada uma entrada de log resumindo cada mecanismo da Web.

Observação: Por padrão, se você não especificar nenhum parâmetro, pdm_webstat exibirá os dados de resumo para todos os processos em execução.

O pdm_webstat retorna zero se o comando for concluído com êxito e um valor diferente de zero se ocorrerem erros (por exemplo, expiração ou nenhum processo de mecanismo da Web ativo).

Exemplo: Saída do pdm_webstat quando nenhum parâmetro for especificado

O exemplo a seguir mostra a saída do pdm_webstat quando executado sem parâmetros:

```
PDM_Webstat: Invoked at 10/11/2007 10:26:42
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
=========================================
Report from Webengine: web:local:1
=========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
```

Importante! Em UNIX, o LIBPATH deve ser definido antes de executar vários utilitários do CA SDM. Use *pdm_task* para definir LIBPATH antes de executar um utilitário. Por exemplo, insira “pdm_task pdm_clean_attachments...".

relatório--Gerar relatórios

Se aplica ao Unix somente

O programa de relatório permite gerar um relatório da linha de comando no servidor. Para emitir o comando report na linha de comando ou em um script, você deve incluir pdm_task. O comando pdm_task configura variáveis de ambiente para comandos que não têm um wrapper. Insira pdm_task com o comando de relatório na mesma linha de comando *somente* quando o relatório for invocado por meio de um script ou da linha de comando. Se você emitir o comando report de um menu, não precisa incluir pdm_task, porque todas as variáveis de ambiente são definidas pelo aplicativo.

Sintaxe

Esse comando apresenta o seguinte formato:

```
pdm_task report [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command line arguments]
```

-e

Echoes compiled script (para fins de depuração).

-f

Usa form-feed entre páginas.

-F ffstring

Define a seqüência de caracteres opcional de form-feed.

-p pagelength

Define o comprimento de página. O comprimento de página padrão é 66.

filename

O modelo de relatório. Se você não estiver executando o comando report do diretório em que o arquivo de modelo está localizado, inclua o nome completo do caminho do arquivo. O comando envia a saída como saída padrão (stdout).

argumentos de linha de comando

Especifica parâmetros recebidos pelo modelo de relatório. Se o relatório é projetado para aceitar argumentos de linha de comando, você deve informar um argumento de linha de comando para cada parâmetro no modelo de relatório. Se o argumento estiver vazio, digite a seqüência de caracteres nula.

Por exemplo, o seguinte comando fornece os argumentos de linha de comando Smith, Jane e L. O modelo de relatório exige estes três parâmetros para gerar o Relatório de contatos afetados.

Por exemplo, digite:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

No próximo exemplo, Jane Smith não tem uma inicial no meio:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Smith Jane "
```

rpt_srv--Generate Reports

Válido apenas para Windows

O programa de relatório permite gerar um relatório da linha de comando no servidor. Para emitir o comando report na linha de comando ou em um script, você deve incluir pdm_task. O comando pdm_task configura variáveis de ambiente para comandos que não têm um wrapper. Insira pdm_task com o comando de relatório na mesma linha de comando somente quando o relatório for invocado por meio de um script ou da linha de comando. Se você emitir o comando report de um menu, não precisa incluir pdm_task, porque todas as variáveis de ambiente são definidas pelo aplicativo.

Sintaxe

Esse comando apresenta o seguinte formato:

```
rpt_srv –m [-h] [-e] [-f] [-F ffstring] [-p pagelength] [-C] [-B] filename [
command line arguments]
```

-m

Significa que o relatório está sendo executado manualmente a partir da linha de comando.

-e

Echoes compiled script (para fins de depuração).

-f

Usa form-feed entre páginas.

-F *ffstring*

Define a seqüência de caracteres opcional de form-feed.

-p *pagelength*

Define o comprimento de página. O comprimento de página padrão é 66.

-C

Altera a codificação de UTF-8 para outro conjunto de caracteres. A saída padrão é UTF-8.

Exemplo: para converter a saída para JIS, você executaria "-C iso-2022-jp"

Exemplo: para codificar para o conjunto de caracteres nativo do sistema operacional, use "DEFAULT" ou "NATIVE".

-B

Suprime a marca de requisição de byte se a variável NX_ADD_UTF8_BYTE_ORDER_MARK for definida.

A opção NX_ADD_UTF8_BYTE_ORDER_MARK é uma assinatura em um arquivo. Permite que os editores que oferecem suporte a UTF-8 mantenham a integridade do UTF-8 do arquivo.

Observação: isso é necessário apenas para dados não ASCII. Se não estiver instalado, o comportamento padrão omite a BOM. Se instalado, defina-o como "1" ou "Sim".

filename

Especifica o modelo do relatório. Se você não estiver executando o comando report do diretório em que o arquivo de modelo está localizado, inclua o nome completo do caminho do arquivo. O comando envia a saída como saída padrão (stdout).

argumentos de linha de comando

Especifica parâmetros recebidos pelo modelo de relatório. Se o relatório é projetado para aceitar argumentos de linha de comando, você deve informar um argumento de linha de comando para cada parâmetro no modelo de relatório. Se o argumento estiver vazio, digite a seqüência de caracteres nula.

Por exemplo, o seguinte comando fornece os argumentos de linha de comando Smith, Jane e L. O modelo de relatório exige estes três parâmetros para gerar o Relatório de contatos afetados.

Por exemplo, digite o seguinte comando:

```
rpt_srv –m c:\reports\affected.rpt Smith Jane L
```

No próximo exemplo, Jane Smith não tem uma inicial no meio:

```
rpt_srv –m c:\reports\affected.rpt Smith Jane "
```

uniconv--Iniciar o daemon conversor de eventos do CA NSM para UNIX

Se aplica ao Unix somente

Quando o CA SDM é integrado com o CA NSM, é possível usar o uniconv para enviar dados de evento genéricos para filtrar daemons no CA SDM. O uniconv é usado em uma ação de mensagem no Gerenciamento de eventos do CA NSM.

Sintaxe

Esse comando apresenta o seguinte formato:

```
uniconv –h &opnode –e &’text’ [-n &

nodeid] [-u &userid] [-d &datem] [-t &’

time’]
```

Restrições

O uniconv deve ser executado a partir do $NX_ROOT/bin no Unix. Para usar esse utilitário, seu local deve estar integrado ao CA NSM.

-h &opnode

Especifica o nome do nó da máquina na qual você está executando o uniconv (obrigatório).

-e &'text'

Especifica o texto completo da mensagem (obrigatório).

-n &nodeid

Especifica o nome do nó a partir do qual a mensagem foi originada (obrigatório).

-u &userid

Especifica a ID de logon da pessoa que originou a mensagem.

-d &datem

Especifica a data do sistema no formato *mm*/*dd*/ *aa*.

-t &'time'

Especifica a hora do sistema.

Grupo de formulários de cliente

Os seguintes formulários da web estão incluídos nos grupos de formulários de cliente:

- about.htmpl
- bin_form_np.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- issue_status_change.htmpl
- list_iss.htmpl
- list_isscat.htmpl
- list_KD.htmpl
- menu_frames.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Grupo de formulários de funcionário

Os seguintes formulários da web estão incluídos nos grupos de formulários de funcionário:

- about.htmpl
- bin_form_np.htmpl
- buttons.htmpl
- change_status_change.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_alg.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_cr.htmpl
- detail_in.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- list_chg.htmpl
- list_chgcat.htmpl
- list_cr.htmpl
- list_in.htmpl
- list_KD.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl
- list_pcat_in.htmpl
- menu_frames.htmpl
- request_status_change.htmpl
- show_error.htmpl
- std_body.htmpl

- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Grupo Formulários do analista

Os seguintes formulários da web estão incluídos nos grupos Formulários do analista:

A

- about.htmpl
- acctyp_role_tab.htmpl
- acctyp_web_auth_tab.htmpl
- acctyp_wsp_tab.htmpl
- admin_empty.htmpl
- admin_main_role.htmpl
- admin_tab_dflt.htmpl
- admin_tree.htmpl
- attmnt_content_tab.htmpl
- attmnt_fields.htmpl
- attmnt_permissions_tab.htmpl
- attmnt_upload_popup.htmpl
- att_mgs_event.htmpl
- att_stype_event.htmpl
- aty_chg_ntfr_tab.htmpl
- aty_chg_svy_tab.htmpl
- aty_cr_ntfr_tab.htmpl
- aty_cr_svy_tab.htmpl
- aty_iss_ntfr_tab.htmpl
- aty_iss_svy_tab.htmpl
- aty_kdComment_ntfr_tab.htmpl
- aty_kd_ntfr_tab.htmpl
- aty_mgs_ntfr_tab.htmpl

B

- bhvtpl_todo_tab.htmpl
- bhvtpl_trans_info_tab.htmpl

- bin_form_np.htmpl

F

- cancel.htmpl
- cancel_empty.htmpl
- category_content_tab.htmpl
- category_permissions_tab.htmpl
- chgcat_auto_assignment_tab.htmpl
- chgcat_prptpl_tab.htmpl
- chgcat_wftpl_tab.htmpl
- chg_accumulate.htmpl
- chg_causedreq_tab.htmpl
- chg_close_all_child.htmpl
- chg_expedite.htmpl
- chg_lr.htmpl
- chg_relchg_tab.htmpl
- chg_relreq_tab.htmpl
- cia_bmhier_tab.htmpl
- cia_export_bmhier.htmpl
- cia_export_nr.htmpl
- cia_nr_tab.htmpl
- cia_pwd_tab.htmpl
- cia_sync_stat.htmpl
- cnote_tracker.htmpl
- cnt_addr_tab.htmpl
- cnt_auto_assignment_tab.htmpl
- cnt_env_tab.htmpl
- cnt_grp_tab.htmpl
- cnt_mem_tab.htmpl
- cnt_notif_tab.htmpl
- cnt_org_tab.htmpl

- cnt_rem_tab.htmpl
- cnt_role_tab.htmpl
- cr_attach_chg.htmpl
- cr_close_all_child.htmpl
- cr_detach_chg.htmpl
- cr_lr.htmpl
- cr_relreq_tab.htmpl

D

- dcon_constraint_tab.htmpl
- dcon_sql_tab.htmpl
- detail.template
- detail_acctyp.htmpl
- detail_act_type_assoc.htmpl
- detail_ADMIN_TREE.htmpl
- detail_alg.htmpl
- detail_arcpur_rule.htmpl
- detail_asset.htmpl
- detail_atev.htmpl
- detail_atomic_cond.htmpl
- detail_attmnt_edit.htmpl
- detail_attmnt_error.htmpl
- detail_attmnt_folder.htmpl
- detail_attmnt_ro.htmpl
- detail_attr_alias.htmpl
- detail_aty.htmpl
- detail_audlog.htmpl
- detail_bhvtpl.htmpl
- detail_bmcls.htmpl
- detail_bmhier.htmpl
- detail_bmrep.htmpl

- detail_BU_TRANS.htmpl
- detail_ca_cmpny.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_chgcat.htmpl
- detail_chgstat.htmpl
- detail_chgtype.htmpl
- detail_CI_ACTIONS.htmpl
- detail_CI_ACTIONS_ALTERNATE.htmpl
- detail_CI_DOC_TEMPLATES.htmpl
- detail_CI_STATUSES.htmpl
- detail_CI_WF_TEMPLATES.htmpl
- detail_cmth.htmpl
- detail_cnote.htmpl
- detail_cnt.htmpl
- detail_cost_cntr.htmpl
- detail_country.htmpl
- detail_cr.htmpl
- detail_crs.htmpl
- detail_crsq.htmpl
- detail_cr_prptpl.htmpl
- detail_ctab.htmpl
- detail_ctimer.htmpl
- detail_ctp.htmpl
- detail_dcon.htmpl
- detail_dept.htmpl
- detail_dmn.htmpl
- detail_doc_rep.htmpl
- detail_DOC_VERSIONS.htmpl
- detail_EBR_ACRONYMS.htmpl
- detail_EBR_LOG.htmpl

- detail_EBR_NOISE_WORDS.htmpl
- detail_EBR_SYNONYMS_ADM.htmpl
- detail_event_log.htmpl
- detail_evt.htmpl
- detail_fmgrp.htmpl
- detail_grc.htmpl
- detail_g_cnt.htmpl
- detail_g_loc.htmpl
- detail_g_org.htmpl
- detail_g_prod.htmpl
- detail_g_qname.htmpl
- detail_g_srvrs.htmpl
- detail_g_tblmap.htmpl
- detail_g_tblrule.htmpl
- detail_help_set.htmpl
- detail_hier_edit.htmpl
- detail_hier_ro.htmpl
- detail_ical_event_template.htmpl
- detail_imp.htmpl
- detail_in.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_isscat.htmpl
- detail_issstat.htmpl
- detail_iss_wf.htmpl
- detail_kc.htmpl
- detail_KCAT.htmpl
- detail_KD.htmpl
- detail_KD_FILE.htmpl
- detail_KD_QA.htmpl
- detail_KD_SAVE_AS.htmpl

- detail_KD_TASK.htmpl
- detail_KD_TASK_cancel_rework.htmpl
- detail_KD_TASK_retire.htmpl
- detail_KD_template.htmpl
- detail_KEIT_TEMPLATES.htmpl
- detail_KT_ACT_CONTENT.htmpl
- detail_KT_BLC.htmpl
- detail_KT_FILE_TYPE.htmpl
- detail_KT_FLG_TYPE.htmpl
- detail_ldap.htmpl
- detail_ldap_group.htmpl
- detail_loc.htmpl
- detail_LONG_TEXTS.htmpl
- detail_lr_ro.htmpl
- detail_macro.htmpl
- detail_macro_type.htmpl
- detail_menu_bar.htmpl
- detail_menu_tree_name.htmpl
- detail_mfrmod.htmpl
- detail_mgs.htmpl
- detail_mgsalg.htmpl
- detail_mgsstat.htmpl
- detail_NOTIFICATION.htmpl
- detail_no_contract_sdsc.htmpl
- detail_nr.htmpl
- detail_nrf.htmpl
- detail_nr_com.htmpl
- detail_ntfl.htmpl
- detail_ntfm.htmpl
- detail_ntfr.htmpl
- detail_options.htmpl

- detail_org.htmpl
- detail_O_COMMENTS.htmpl
- detail_O_EVENTS.htmpl
- detail_pcat.htmpl
- detail_perscnt.htmpl
- detail_position.htmpl
- detail_pr.htmpl
- detail_prefs.htmpl
- detail_pri.htmpl
- detail_prod.htmpl
- detail_projex.htmpl
- detail_prptpl.htmpl
- detail_prpval.htmpl
- detail_prpval_rule.htmpl
- detail_prp_edit.htmpl
- detail_QUERY_POLICY.htmpl
- detail_rc.htmpl
- detail_response.htmpl
- detail_role.htmpl
- detail_role_go_form.htmpl
- detail_rptmeth.htmpl
- detail_rrf.htmpl
- detail_rss.htmpl
- detail_sapolicy.htmpl
- detail_saprobtyp.htmpl
- detail_sdsc.htmpl
- detail_sdsc_map.htmpl
- detail_seq.htmpl
- detail_sev.htmpl
- detail_site.htmpl
- detail_slatpl.htmpl

- detail_srvr_aliases.htmpl
- detail_srvr_zones.htmpl
- detail_state.htmpl
- detail_svc_contract.htmpl
- detail_svy_atpl.htmpl
- detail_svy_qtpl.htmpl
- detail_svy_tpl.htmpl
- detail_tab.htmpl
- detail_tenant.htmpl
- detail_tenant_group.htmpl
- detail_tskstat.htmpl
- detail_tskty.htmpl
- detail_tspan.htmpl
- detail_typecnt.htmpl
- detail_tz.htmpl
- detail_urg.htmpl
- detail_USP_PREFERENCES.htmpl
- detail_usp_servers.htmpl
- detail_vpt.htmpl
- detail_web_form.htmpl
- detail_wf.htmpl
- detail_wftpl.htmpl
- detail_wrkshft.htmpl
- dmn_dcon_tab.htmpl
- edit_prop_dyn.htmpl
- ed_image_pane.htmpl
- evt_action_info.htmpl
- evt_config_info.htmpl

I

- generic.htmpl

- get_comment.htmpl
- g_profile_browser.htmpl
- g_profile_browser2.htmpl
- g_profile_browser3.htmpl
- g_profile_browser_frameset.htmpl
- g_profile_jump.htmpl
- g_profile_scratchpad.htmpl

h

- hierload_admin_tree.htmpl
- hierload_KCAT.htmpl
- hiersel_admin_tree.htmpl
- hiersel_KCAT.htmpl
- hourglass.htmpl
- html_editor_create_change_order.htmpl
- html_editor_create_ticket.htmpl
- html_editor_frames.htmpl
- html_editor_insert_image.htmpl
- html_editor_insert_link.htmpl
- html_editor_insert_table.htmpl
- html_editor_tabs.htmpl
- html_editor_toolbar.htmpl

I

- insert_iss_wf.htmpl
- insert_wf.htmpl
- in_relreq_tab.htmpl
- isscat_auto_assignment_tab.htmpl
- isscat_prptpl_tab.htmpl
- isscat_wftpl_tab.htmpl
- issue_status_change.htmpl
- iss_accumulate.htmpl

- iss_close_all_child.htmpl
- iss_custfld_tab.htmpl
- iss_expedite.htmpl
- iss_lr.htmpl
- iss_reliss_tab.htmpl
- iss_resol_tab.htmpl

K

- kd_action_forward.htmpl
- kd_action_publish.htmpl
- kd_action_reject.htmpl
- kd_action_unpublish.htmpl
- kd_action_unretire.htmpl
- kd_attachments_tab.htmpl
- kd_attributes_tab.htmpl
- kd_categories_tab.htmpl
- kd_content_tab.htmpl
- kd_file_prop_tab.htmpl
- kd_permissions_tab.htmpl
- kd_qa_attributes_tab.htmpl
- kd_qa_content_tab.htmpl
- keit_tmpl_export_fields_tab.htmpl
- keit_tmpl_export_filter_tab.htmpl
- keit_tmpl_import_settings_tab.htmpl
- keit_tmpl_name_tab.htmpl
- kt_admin_attachments.htmpl
- kt_admin_automated_policies.htmpl
- kt_admin_document_settings.htmpl
- kt_admin_faq_options.htmpl
- kt_admin_general_settings.htmpl
- kt_admin_integration.htmpl

- kt_admin_knowledge.htmpl
- kt_admin_parse_settings.htmpl
- kt_admin_report_card.htmpl
- kt_admin_search_config_cr.htmpl
- kt_admin_search_config_iss.htmpl
- kt_admin_search_options.htmpl
- kt_admin_survey_settings.htmpl
- kt_admin_workflow_settings.htmpl
- kt_architect.htmpl
- kt_architect2.htmpl
- kt_architect3.htmpl
- kt_architect_delete_KCAT.htmpl
- kt_architect_delete_KD.htmpl
- kt_architect_frameset.htmpl
- kt_architect_init.htmpl
- kt_architect_javascript.htmpl
- kt_architect_KCATs.htmpl
- kt_architect_KCAT_path.htmpl
- kt_architect_KDs.htmpl
- kt_dtbuilder.htmpl
- kt_dtbuilder2.htmpl
- kt_dtbuilder3.htmpl
- kt_dtbuilder_frameset.htmpl
- kt_dtbuilder_node.htmpl
- kt_dtbuilder_prompt_window.htmpl
- kt_dtbuilder_save_dialog_window.htmpl
- kt_dtbuilder_save_tree_form.htmpl
- kt_dtbuilder_tree.htmpl
- kt_email_document.htmpl
- kt_faq_tree.htmpl
- kt_main.htmpl

- kt_main2.htmpl
- kt_main3.htmpl
- kt_main_role.htmpl
- kt_permissions.htmpl

L

- list.template
- list_acctyp.htmpl
- list_act_type_assoc.htmpl
- list_alg.htmpl
- list_all_fmgrp.htmpl
- list_all_lr.htmpl
- list_architect_KDs.htmpl
- list_architect_KDs_Pref.htmpl
- list_arcpur_hist.htmpl
- list_arcpur_rule.htmpl
- list_atev.htmpl
- list_atomic_cond.htmpl
- list_attmnt.htmpl
- list_attr_alias.htmpl
- list_aty.htmpl
- list_audlog.htmpl
- list_bmcls.htmpl
- list_bmhier.htmpl
- list_bmrep.htmpl
- list_bm_task.htmpl
- list_bool.htmpl
- list_ca_cmpny.htmpl
- list_ca_logical_asset.htmpl
- list_chg.htmpl
- list_chgalg.htmpl

- list_chgcat.htmpl
- list_chgsched.htmpl
- list_chgsched_config.htmpl
- list_chgstat.htmpl
- list_chgtype.htmpl
- list_CI_ACTIONS.htmpl
- list_CI_ACTIONS_ALTERNATE.htmpl
- list_CI_DOC_TEMPLATES.htmpl
- list_CI_STATUSES.htmpl
- list_CI_WF_TEMPLATES.htmpl
- list_cmth.htmpl
- list_cnote.htmpl
- list_cnt.htmpl
- list_cost_cntr.htmpl
- list_country.htmpl
- list_cr.htmpl
- list_crs.htmpl
- list_crsq.htmpl
- list_crs_cr.htmpl
- list_crs_in.htmpl
- list_crs_pr.htmpl
- list_crt.htmpl
- list_cr_kt.htmpl
- list_ctab.htmpl
- list_ctimer.htmpl
- list_ctp.htmpl
- list_dcon.htmpl
- list_dept.htmpl
- list_dmn.htmpl
- list_DOC_VERSIONS.htmpl
- list_EBR_ACRONYMS.htmpl

- list_EBR_LOG.htmpl
- list_EBR_NOISE_WORDS.htmpl
- list_EBR_SYNONYMS_ADM.htmpl
- list_event_log.htmpl
- list_evt.htmpl
- list_evtdly.htmpl
- list_grc.htmpl
- list_grpmem.htmpl
- list_g_chg_queue.htmpl
- list_g_cnt.htmpl
- list_g_cr_queue.htmpl
- list_g_iss_queue.htmpl
- list_g_loc.htmpl
- list_g_org.htmpl
- list_g_prod.htmpl
- list_g_qname.htmpl
- list_g_srvrs.htmpl
- list_g_tblmap.htmpl
- list_g_tblrule.htmpl
- list_g_tenant.htmpl
- list_help_item.htmpl
- list_help_set.htmpl
- list_ical_event_template.htmpl
- list_imp.htmpl
- list_in.htmpl
- list_iss.htmpl
- list_issalg.htmpl
- list_isscat.htmpl
- list_issstat.htmpl
- list_iss_kt.htmpl
- list_iss_wf.htmpl

- list_kc.htmpl
- list_KCAT_LINKED.htmpl
- list_KCAT_QA.htmpl
- list_KCAT_tree.htmpl
- list_KD.htmpl
- list_kdsched.htmpl
- list_kdsched_config.htmpl
- list_KD_ATTMNT.htmpl
- list_kd_CI_DOC_LINKS.htmpl
- list_KD_FILE.htmpl
- list_kd_INDEX_DOC_LINKS.htmpl
- list_KD_QA.htmpl
- list_KEIT_export_transactions.htmpl
- list_KEIT_IMPORT_PACKAGES.htmpl
- list_KEIT_import_transactions.htmpl
- list_KEIT_TEMPLATES.htmpl
- list_KT_ACT_CONTENT.htmpl
- list_KT_BLC.htmpl
- list_KT_FILE_TYPE.htmpl
- list_KT_FLG_TYPE.htmpl
- list_KT_FREE_TEXT.htmpl
- list_KT_LIFE_CYCLE_REP.htmpl
- list_ldap.htmpl
- list_ldap_group.htmpl
- list_loc.htmpl
- list_LONG_TEXTS.htmpl
- list_lr.htmpl
- list_macro.htmpl
- list_macro_type.htmpl
- list_menu_bar.htmpl
- list_menu_tree_name.htmpl

- list_mfrmod.htmpl
- list_mgs.htmpl
- list_mgsalg.htmpl
- list_mgsstat.htmpl
- list_NOTIFICATION.htmpl
- list_no_contract_sdsc.htmpl
- list_nr.htmpl
- list_nrf.htmpl
- list_nr_com.htmpl
- list_ntfl.htmpl
- list_ntfm.htmpl
- list_ntfr.htmpl
- list_OA_TABLES.htmpl
- list_options.htmpl
- list_org.htmpl
- list_O_EVENTS.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl
- list_pcat_in.htmpl
- list_pcat_pr.htmpl
- list_perscnt.htmpl
- list_position.htmpl
- list_pr.htmpl
- list_pri.htmpl
- list_prod.htmpl
- list_prod_list.htmpl
- list_prpval.htmpl
- list_prpval_rule.htmpl
- list_QUERY_POLICY.htmpl
- list_QUERY_POLICY_ACTIONS.htmpl
- list_rc.htmpl

- list_rel_cat.htmpl
- list_response.htmpl
- list_role.htmpl
- list_role_tab.htmpl
- list_rptmeth.htmpl
- list_rrf.htmpl
- list_rss.htmpl
- list_sapolicy.htmpl
- list_saprobtyp.htmpl
- list_sdsc.htmpl
- list_sdsc_map.htmpl
- list_seq.htmpl
- list_sev.htmpl
- list_showgrp.htmpl
- list_site.htmpl
- list_srvr_aliases.htmpl
- list_srvr_zones.htmpl
- list_state.htmpl
- list_svc_contract.htmpl
- list_svy_atpl.htmpl
- list_svy_qtpl.htmpl
- list_svy_tpl.htmpl
- list_tab.htmpl
- list_tenant.htmpl
- list_tenant_group.htmpl
- list_tskstat.htmpl
- list_tskty.htmpl
- list_tspan.htmpl
- list_typecnt.htmpl
- list_tz.htmpl
- list_urg.htmpl

- list_usp_servers.htmpl
- list_vpt.htmpl
- list_web_form.htmpl
- list_wf.htmpl
- list_wrkshft.htmpl
- load_properties.htmpl
- load_wait.htmpl
- loc_address_tab.htmpl
- loc_auto_assignment_tab.htmpl
- log_reader.htmpl
- log_reader_banner.htmpl
- log_reader_fs.htmpl
- log_sol_4itil.htmpl

m

- macro_atomic_cond_tab.htmpl
- macro_cnt_tab.htmpl
- macro_ctp_tab.htmpl
- macro_ntfl_tab.htmpl
- macro_rrf_tab.htmpl
- mactyp_execscript_tab.htmpl
- mactyp_valscript_tab.htmpl
- mapped_contracts_tab.htmpl
- menubar.template
- menubar_admin.htmpl
- menubar_architect.htmpl
- menubar_chg_sched.htmpl
- menubar_dtbuilder.htmpl
- menubar_html_editor.htmpl
- menubar_kt.htmpl
- menubar_no.htmpl

- menubar_sd.htmpl
- menubar_sd_chg_manager.htmpl
- menubar_sd_cust_mgr.htmpl
- menubar_sd_cust_rep.htmpl
- menubar_sd_hd_manager.htmpl
- menubar_sd_inc_manager.htmpl
- menubar_sd_know_analyst.htmpl
- menubar_sd_know_manager.htmpl
- menubar_sd_l1_analyst.htmpl
- menubar_sd_l2_analyst.htmpl
- menubar_sd_prb_manager.htmpl
- menubar_sd_vendor_analyst.htmpl
- menu_frames.htmpl
- menu_tree_editor.htmpl
- menu_tree_editor2.htmpl
- menu_tree_editor3.htmpl
- mgs_cnt_tab.htmpl
- mgs_ctp_tab.htmpl
- mgs_ini_tab.htmpl
- mgs_ntfl_tab.htmpl
- mgs_rem_tab.htmpl
- multiframe.template
- multiframe_reports_admin.htmpl
- multiframe_reports_chg_manager.htmpl
- multiframe_reports_cust_mgr.htmpl
- multiframe_reports_inc_mgr.htmpl
- multiframe_reports_know_analyst.htmpl
- multiframe_reports_know_mgr.htmpl
- multiframe_reports_prb_mgr.htmpl
- multiframe_reports_sd_mgr.htmpl

N

- new_lr.htmpl
- nf.htmpl
- nosession.htmpl
- nr_bm_tab.htmpl
- nr_chg_tab.htmpl
- nr_contact_tab.htmpl
- nr_inc_tab.htmpl
- nr_inv_tab.htmpl
- nr_iss_tab.htmpl
- nr_loc_tab.htmpl
- nr_log_tab.htmpl
- nr_org_tab.htmpl
- nr_prb_tab.htmpl
- nr_projex_tab.htmpl
- nr_rel_tab.htmpl
- nr_reqitil_tab.htmpl
- nr_req_tab.htmpl
- nr_serv_tab.htmpl
- ntfl_ntfr_tab.htmpl
- ntfr_aty_tab.htmpl
- ntfr_cnt_tab.htmpl
- ntfr_ctp_tab.htmpl
- ntfr_ntfl_tab.htmpl

D

- order_status_change.htmpl
- org_address_tab.htmpl
- org_env_tab.htmpl

P

- pcat_auto_assignment_tab.htmpl

- pcat_prptpl_tab.htmpl
- pcat_wftpl_tab.htmpl
- power_user_tips.htmpl
- profile_browser.htmpl
- profile_browser2.htmpl
- profile_browser3.htmpl
- profile_browser_frameset.htmpl
- profile_envcnt.htmpl
- profile_envorg.htmpl
- profile_histcnt_chg.htmpl
- profile_histcnt_cr.htmpl
- profile_histcnt_in.htmpl
- profile_histcnt_iss.htmpl
- profile_histcnt_pr.htmpl
- profile_historg_chg.htmpl
- profile_historg_cr.htmpl
- profile_historg_in.htmpl
- profile_historg_iss.htmpl
- profile_historg_pr.htmpl
- profile_infocnt.htmpl
- profile_infoorg.htmpl
- profile_menu.htmpl
- profile_qtemplate.htmpl
- pr_attinc_tab.htmpl
- pr_relreq_tab.htmpl

S

- reports.htmpl
- reports.htmpl.tpl
- request_status_change.htmpl
- role_auth_tab.htmpl

- role_fnacc_tab.htmpl
- role_goform_tab.htmpl
- role_kt_ct_tab.htmpl
- role_kt_docs_tab.htmpl
- role_webform_tab.htmpl
- role_web_interface_tab.htmpl

s

- sapolicy_ac_tab.htmpl
- sapolicy_pt_tab.htmpl
- saprobtyp_dh_tab.htmpl
- saprobtyp_rd_tab.htmpl
- scoreboard.htmpl
- scratchpad.htmpl
- screen_reader_usage.htmpl
- sdsc_chg_slatpl_tab.htmpl
- sdsc_chg_wf_slatpl_tab.htmpl
- sdsc_cr_slatpl_tab.htmpl
- sdsc_iss_slatpl_tab.htmpl
- sdsc_iss_wf_slatpl_tab.htmpl
- sdsc_map_cnt_tab.htmpl
- sdsc_map_grp_tab.htmpl
- sdsc_map_nr_tab.htmpl
- sdsc_map_pri_tab.htmpl
- sdsc_map_urg_tab.htmpl
- sd_kt_admin.htmpl
- sd_main.htmpl
- sd_main_role.htmpl
- search_child_KCATs_filter.htmpl
- show_error.htmpl
- show_main_detail.htmpl

- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_head_site.htmpl
- suggest_knowledge_isscat.htmpl
- suggest_knowledge_list_isscat.htmpl
- suggest_knowledge_list_pcat.htmpl
- suggest_knowledge_pcat.htmpl
- sugggest_knowledge_search_options.htmpl

T

- tab_detail.template
- tenant_address_tab.htmpl
- tenant_groups_tab.htmpl
- tenant_group_members_tab.htmpl
- tskty_tskstat_tab.htmpl

U

- update_lrel_bmrep.htmpl
- update_lrel_chg.htmpl
- update_lrel_chgcat.htmpl
- update_lrel_cnt.htmpl
- update_lrel_cr.htmpl
- update_lrel_ctp.htmpl
- update_lrel_goform.htmpl
- update_lrel_help_content.htmpl
- update_lrel_in.htmpl
- update_lrel_iss.htmpl
- update_lrel_isscat.htmpl
- update_lrel_loc.htmpl

- update_lrel_macro.htmpl
- update_lrel_nr.htmpl
- update_lrel_ntfl.htmpl
- update_lrel_ntfr.htmpl
- update_lrel_org.htmpl
- update_lrel_pcat.htmpl
- update_lrel_pr.htmpl
- update_lrel_role.htmpl
- update_lrel_tab.htmpl
- update_lrel_tenant.htmpl
- update_lrel_tenant_group.htmpl
- update_lrel_tskstat.htmpl
- update_lrel_webform.htmpl
- update_lrel_wrkshft.htmpl
- upd_chg_sched.htmpl
- upload_file.htmpl
- upload_success.htmpl
- usq_update.htmpl
- usq_update_control.htmpl
- usq_update_fin.htmpl
- usq_update_select.htmpl
- usq_update_tree.htmpl

V

- v30_date_helper.htmpl

W

- wfdef.htmpl
- wftpl_auto_assignment_tab.htmpl
- wftpl_bhvtpl_tab.htmpl
- working.htmpl
- workitems.htmpl

- wrkshft_auto_assignment_tab.htmpl
- wrkshft_schedule_tab.htmpl
- wspmain.htmpl

v

- xfer_esc_chg.htmpl
- xfer_esc_cr.htmpl
- xfer_esc_iss.htmpl
- xx_attmnt_tab.htmpl
- xx_candp_tab.htmpl
- xx_nr_tab.htmpl
- xx_prop_tab.htmpl
- xx_solnalg_tab.htmpl
- xx_stype_tab.htmpl
- xx_template_tab.htmpl
- xx_wf_tab.htmpl

Apêndice E: Solução de problemas de desempenho

Identificação de problemas de desempenho no CA SDM

Os clientes que tiverem problemas de desempenho no CA SDM podem coletar informações sobre seu ambiente antes de entrar em contato com o Suporte online da CA para ajudar a identificar e resolver problemas do CA SDM. Use a Ferramenta de relatórios de diagnóstico do CA SDM e o Script de registro de intervalos para coletar informações de diagnóstico sobre o ambiente do CA SDM. Por exemplo, entenda a configuração do computador para determinar o tipo de sistema operacional, versão e os recursos disponíveis do sistema.

Importante: Instale e configure o servidor do CA SDM antes de executar a ferramenta de diagnóstico. Execute o utilitário de diagnóstico em todas as instalações de servidor primário e secundário do CA SDM. A ferramenta *não* altera ou modifica o servidor do CA SDM.

Observação: recomendamos que você entre em contato com o Suporte online da CA antes de usar a ferramenta de diagnóstico.

O processo a seguir descreve como identificar problemas de desempenho:

1. Definir o problema de desempenho. (na página 1240)
2. Colete os seguintes dados de ambiente específicos do local:
   - Execute a ferramenta do Relatório de Diagnósticos do CA SDM (na página 1241).
     - Relatório do Windows
     - Relatório do UNIX

- Relatório de diagnóstico coletado

- Colete detalhes do ambiente do servidor de banco de dados (na página 1249).
- Colete topologia de rede e informações de topologia ou outros produtos que se integram com o CA SDM.

  Por exemplo, localize as informações sobre produtos de arquivos PDF ou diagramas disponíveis.

3. Executar o script de log do intervalo (na página 1247).
4. Examine as recomendações gerais de ajuste (na página 1249).

Defina o problema de desempenho

Defina o problema de desempenho coletando, inicialmente, informações do sistema. Examine a lista de perguntas para determinar se elas são relevantes para o seu problema. Os seguintes exemplos de perguntas podem ajudá-lo a definir o problema.

- Que problema fez com que os usuários interrompessem suas tarefas?
- Quando detectaram o problema pela primeira vez?
- O ambiente passou por alguma mudança recente, por exemplo a atualização de hardware?
- Que funcionalidade do produto enfrenta problemas?
- Quantos usuários e que tipo de usuários o problema afetou?
- Quais usuários não são afetados?
- Qual é a localização geográfica do usuário que percebe o problema?
- Qual é o nível de acesso dos usuários afetados?
- Hospeda o CA SDM em um servidor VMWare ESX ou outros ambientes virtualizados?
- Que outro software está em execução no servidor ESX ou computador host?
- Quais são as especificações desse ambiente?
- Quantas CPUs possui em cada computador?
- Quanta memória foi configurada para cada computador?

Usar a Ferramenta de relatórios de diagnóstico da CA

É possível usar a ferramenta de diagnóstico com sistema operacional Windows, Oracle Solares, AIX e Linux. Após executar supp_diag, a ferramenta detecta o tipo de sistema operacional para determinar quais comandos utilizar para a coleta de dados da instalação do CA SDM.

A ferramenta cria um arquivo .CAZ no sistema operacional Windows e um arquivo .tar.gz no UNIX no diretório que você carrega com a ocorrência para o site http://support.ca.com.

Windows

Defina $NX_ROOT como o diretório raiz da instalação do CA SDM. A localização padrão de $NX_ROOT é C:\Arquivos de programas\CA\Service Desk\ no Windows. É possível alterar o padrão quando você deseja alterar o diretório padrão durante o processo de instalação.

Importante: A ferramenta de diagnóstico requer o pslist.exe para executar corretamente no Windows. Baixa a pslist do site de suporte da Microsoft. Instale a pslist no CA SDM e adicione o caminho do diretório variável para a variável de caminho do sistema antes de usar a ferramenta de diagnóstico.

UNIX/Linux

Defina $NX_ROOT como o diretório raiz da instalação do CA SDM. O padrão de $NX_ROOT é /opt/CAisd/ em um sistema operacional UNIX ou Linux. É possível alterar o padrão quando você deseja alterar o diretório padrão durante o processo de instalação.

Siga estas etapas:

1. Realize uma da seguintes ações:
   - No Windows, verifique se a variável de caminho do sistema inclui $NX_ROOT\bin.
   - No UNIX, verifique se o seu $PATH inclui $NX_ROOT/bin.
2. No Windows, execute supp_diag.cmd ; no UNIX, execute supp_diag.sh.

   A ferramenta de diagnóstico pode levar de 5 a 10 minutos para ser concluída.

3. Se o processo de coleta de dados não for concluído, exiba o arquivo de log $NX_ROOT\diag\<host_name>_supp_diag.log para determinar os erros ao coletar informações de diagnóstico.

   Observação: se deseja cancelar o trabalho em lote em segundo plano, utilize CTRL-C para cancelar o arquivo em lote. Alguns processos ainda executarão no segundo plano, como MSINFO32.exe. Se tiver dúvidas sobre o uso dessa ferramenta de diagnóstico, entre em contato com o Suporte online da CA.

4. A estrutura de diretórios do script exibirá o local dos arquivos de script, arquivos zip de diagnóstico e arquivos de log:

   - O diretório $NX_ROOT\diag\bin contém arquivos de script.
   - O diretório $NX_ROOT\diag\rpt contém o arquivo zip de diagnóstico (em formato .caz no Windows e em formato .tar.gz no UNIX).
   - O diretório $NX_ROOT\diag\misc_logs contém os arquivos de log que podem ser automaticamente incluídos no arquivo zip.

5. Conclua as etapas apropriadas para descompactar os arquivos compilados, que têm por base seu sistema operacional:

   Windows

   - Abra um prompt de comando.
   - CD para $NX_ROOT\diag\rpt ou qualquer diretório em que o arquivo .CAZ estiver localizado.
   - Execute o seguinte comando.

   ```
   $NX_ROOT\diag\bin\cazipxp -u <package_name>.CAZ
   ```

   UNIX

   - Abra um prompt de comando.
   - CD para $NX_ROOT/diag/rpt ou qualquer diretório onde o arquivo .tar ou .tar.gz estiver localizado.
   - Descompacte o arquivo:

   ```
   gunzip -d <package_name>.tar.gz
   tar -xvf <package_name>.tar
   ```

Relatório do Windows

A lista a seguir descreve os arquivos de relatório do Windows que são criados e incluídos no pacote do arquivo CAZ\tar.

Ca.olf

Especifica as informações de licenciamento da CA a partir do diretório ca_lic.

Lic98.log

Especifica o arquivo de log que está relacionado ao licenciamento da CA no diretório ca_lic.

Lic98version.log

Especifica o arquivo de log que está relacionado ao licenciamento da CA no diretório ca_lic.

Licdebug.log log

Especifica o arquivo que está relacionado ao licenciamento da CA no diretório ca_lic.

Drwatsoninfo.txt

Especifica a configuração do Dr. Watson no computador.

<host name>_env.txt

Especifica as variáveis de ambiente definidas no computador.

<host name>_slstat.txt

Especifica o resultado do commando slstat.

<host name>_pdm_status.txt

Especifica o resultado do commando slstat.

<host name>_dir_listing.txt

Especifica a listagem de diretório de instalação do Service Desk.

<host name>_pslist.txt

Especifica a listagem de processo quando a ferramenta pslist Micrososim, pfft estiver instalada.

<host name>_MSINFO32.NFO

Especifica as informações do sistema de coleta dos resultados do MSINFO.

<host name>_SYSTEMINFO.TXT

Especifica as informações do sistema.

<host name>_appevents.csv

Especifica os logs de eventos do aplicativo criados nos últimos sete dias.

<host name>_sysevents.csv

Especifica os logs de eventos do aplicativo criados nos últimos sete dias.

<host name>_hostinfo.txt

Especifica as informações do computador.

<host name>_prodinstallinfo.txt

Especifica as informações de instalação dos produtos da CA.

<host name>_caprod_registry.txt

Especifica as informações de registro dos produtos CA instalados.

<host name>_softfeatures.txt

Especifica a lista de recursos de software que estão instalados para o Service Desk.

<host name>_ipconfig.txt

Especifica as informações de configuração de IP.

<host name>_supp_diag.log

Especifica o log criado para a execução da ferramenta supp_diag.

Relatório de UNIX

A lista a seguir descreve os arquivos de relatório do UNIX que são criados e incluídos no arquivo CAZ\tar.

Ca.olf

Especifica as informações de licenciamento da CA a partir do diretório ca_lic.

Lic98.log

Especifica o arquivo de log que está relacionado ao licenciamento da CA no diretório ca_lic.

<host name>_env.txt

Especifica as variáveis de ambiente definidas no computador.

<host name>_slstat.txt

Especifica o resultado do commando slstat.

<host name>_pdm_status.txt

Especifica o resultado do commando slstat.

<host name>_dir_listing.txt

Especifica a listagem de diretório de instalação do Service Desk.

<host name>_pslist.txt

Especifica a listagem de processo quando a ferramenta pslist Microsoft estiver instalada.

<host name>_uname.txt

Especifica o resultado do comando uname do sistema operacional.

<host name>_diskinfo.txt

Especifica o resultado do comando df do sistema operacional.

<host name>_freemem.txt

Especifica o resultado da informações da memória.

<host name>_supp_diag.log

Especifica o log criado para a execução da ferramenta supp_diag.

<host name>_prtconf.txt

Especifica o resultado do comando prtconf do sistema operacional em computadores Solaris e AIX.

<host name>_solrev.txt

Especifica a versão do sistema operacional e as informações de patches em computadores Solaris.

<host name>_netconf.txt

Especifica as informações de configuração de IP em computadores AIX.

Relatório de diagnóstico coletado

A lista de arquivos\diretórios da documentação padrão do CA SDM inclui os seguintes relatórios no arquivo CAZ\tar. Adicione arquivos/diretórios adicionais que incluiu no arquivo CAZ\tar, colocando-o no diretório $NX_ROOT\diag\misc_logs.

- $NX_ROOT/GENLEVEL ou $NX_ROOT/.GENLEVEL
- $NX_ROOT/<COMPUTERNAME>.his
- $NX_ROOT/NX.env

- $NX_ROOT/NX.env.last
- $NX_ROOT/log\
- $NX_ROOT/pdmconf\
- $NX_ROOT/pdmconf\version
- $NX_ROOT/bopcfg\www*.cfg
- $NX_ROOT/site\mods\
- $NX_ROOT/site\ddict.sch
- $NX_ROOT/site\eh\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\logs\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps*.xml

Executar o script de registro em log do intervalo

O registro em log do intervalo determina o uso de recursos no servidor. Confirme se quaisquer processos consomem grandes quantidades da CPU, memória, ou E/S de disco no servidor. O script do Intervalo de Log (arquivo em lotes do Windows Server ou um Shell Script no Unix/Linux) é iniciado automaticamente quando os serviços do Gerenciador do Service Desk iniciam. O script em lotes coleta estatísticas do CA SDM e do sistema operacional a cada 3 minutos.

Para Windows, o arquivo em lote gera a CPUStats _ Hostname.txt, pslistx _ hostname.out, pslistm _ hostname.out, netstat _ hostname.out arquivos para os servidores principal e secundário na pasta $NX_ROOT/log. Apenas para servidores principais, o arquivo em lote gera dbstats_hostname.out e status_hostname.out.

Para UNIX/Linux, o script cria um arquivo chamado interval_log_<hostname>.out na pasta $NX_ROOT/log. O script armazena todos os arquivos de backup na pasta interval_logging com o carimbo de data/hora na pasta $NX_ROOT/log.

Observação: se seu sistema UNIX tiver a ferramenta TOP, adicione essa ferramenta aos conjuntos de comandos de Registro em log interno. Para o Suporte online da CA, tome nota das estatísticas do sistema operacional de saída da ferramenta TOP para os 50 principais processos que ocupam a maior parte dos recursos do sistema.

Para Windows 2008, esse utilitário requer que a ferramenta pslist.exe (parte de pstools.zip) seja instalada e adicionada à variável do ambiente %PATH% do sistema operacional Windows em cada um dos servidores do CA SDM.

Execute as etapas a seguir para fazer o download do PS Tools Suite:

1. Baixe o PS Tools Suite da Microsoft.
2. Extraia pstools.zip para uma pasta de sua escolha e adicione a pasta à variável de ambiente %PATH% do Windows.
3. Executar pslist.exe uma vez manualmente a partir do prompt de comando como o usuário do Sistema Local e aceitar o contrato de licença. Para executar o pslist.exe como o usuário do Sistema Local, execute o seguinte comando:

   ```
   psexec.exe -s -i pslist.exe
   ```

   Observação: é possível iniciar o serviço do Windows do CA SDM em uma conta de usuário diferente que não seja a conta do Sistema Local. Para esse serviço, execute pslist.exe na conta e aceite o contrato de licença. Se pslist.exe é adicionado após a instalação e a configuração do CA SDM, reinicie os serviços do CA SDM depois de aceitar o contrato de licença do pslist.

Coletar detalhes do ambiente do servidor de banco de dados

Colete detalhes sobre o servidor de banco de dados. Essas informações podem ajudar a identificar problemas de desempenho no CA SDM.

Siga estas etapas:

1. Determine o local de seu servidor de banco de dados, como local ou remoto.
2. Determine a versão do DBMS, versão do sistema operacional e nível de patch.
3. Conclua as etapas apropriadas para seu tipo de banco de dados:
   - Execute as seguintes consultas para o SQL Server e observe os resultados:

     ```
     select @@version
     SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel')
     ```

   - Execute a consulta a seguir para Oracle:

     ```
     select * from v$version where banner like 'Oracle%';
     ```

4. Confirme a versão do cliente do banco de dados instalado no servidor de aplicativos.
5. Se disponível, colete mais informações sobre dados de ambiente, como o sistema operacional, outros bancos de dados, e assim por diante.

Examinar as recomendações gerais de ajuste

Recomendamos que você monitore os principais indicadores de desempenho e o consumo de recursos regularmente. Você também pode ajudar a garantir que a manutenção de rotina seja aplicada para ajudar a identificar problemas menores, antes que eles se tornem graves.

Se você suspeita de um problema ou se os usuários reclamarem sobre desempenho lento, abra uma ocorrência no Suporte online da CA, envie o resultado do script de registro em log do intervalo, Ferramenta de diagnóstico do CA SDM, os logs padrão do CA SDM e as informações sobre o problema. Envie essas informações para o Suporte online de cada servidor primário e secundário do CA SDM.

A lista a seguir descreve sinais de problemas de desempenho comuns:

- M~ensagens longas nos logs padrão do CA SDM (arquivos stdlog.x)
- Procure mensagens nos stdlogs que indiquem “A seguinte consulta demorou # # # # milissegundos”.
- Enfileiramento em agentes de banco de dados na saída pdm_vdbinfo
- Procure *Solicitações em fila (#)* na saída pdm_vdbinfo. É possível executar esse comando, manualmente, no prompt do sistema operacional. O script de registro em log do intervalo também executa esse comando.
- Número elevado de usuários conectados a cada mecanismo da web. Por exemplo, há mais de 200 usuários.

  Observação: execute pdm_webstat para exibir o número de usuários simultâneos por mecanismo da web. É possível executar esse comando, manualmente, no prompt do sistema operacional. O script de registro em log do intervalo também executa esse comando.
- Reclamações dos usuários